Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Courbes elliptiques et cryptographie

J. Rostand

R & D pour la défense Canada
MÉMORANDUM TECHNIQUE
DREO TM 2001-095
Octobre 2001

Canada

P517601.PDF [Page: 4 of 64]

105-03244/

Courbes elliptiques et cryptographie

J Rostand

Centre de recherches pour la défense, Ottawa
Mémorandum technique
DREO TM 2001-095
Octobre 2001

Auteur

J Rostand, Ph D.

Approbation scientifique et technique donnée par

M McIntyre
Chef de section / opérations d'information

Autorisation de publier donnée par

G. Marwood
Président du comité de révision des documents

© Sa majesté la reine, représentée par le ministre de la Défense nationale, 2001
© Her Majesty the Queen as represented by the Minister of National Defence, 2001

Résumé

Les techniques de cryptographie à clés publiques sont largement utilisées aujourd'hui pour la protection de données électroniques. L'une de ces techniques, qui est particulièrement prometteuse, est basée sur la théorie des courbes elliptiques. Ce document à pour but de décrire la cryptographie sur courbes elliptiques (ECC)

Nous commencerons par un bref rappel des notions de structures algébriques élémentaires. Puis, nous définirons les concepts de courbes elliptiques et de groupes sur courbes elliptiques, et nous verrons comment ces derniers peuvent être utilisés pour construire un système cryptographique à clés publiques. Nous discuterons ensuite de certaines courbes elliptiques particulières qu'il faut éviter en cryptographie en raison de leur sécurité réduite. Finalement, nous terminerons par une revue des normes internationales qui traitent ou font référence à ECC.

Abstract

Public key cryptography is widely used nowadays for electronic data protection. One of the most promising public key technique is based on the theory of elliptic curves. The objective of this document is to describe elliptic curve cryptography (ECC).

We will start with recalling some basic notions of algebraic structures. Then, we will define the concept of elliptic curves and groups over elliptic curves and we will see how those groups can be used to construct a public key cryptosystem. Thereafter, we will discuss the case of some particular elliptic curves that are known to be insecure in cryptography. Finally, we will wind up with a review of the international standards that are related to ECC.

This page is left blank

This page is left blank

P517601.PDF [Page: 8 of 64]

Sommaire

Depuis l'avènement d'Internet, les communications et les transactions électroniques se font de plus en plus nombreuses. La cryptographie est essentielle pour mettre en place des systèmes d'authentification efficaces et pour obtenir une protection adéquate des données échangées.

La cryptographie sur courbes elliptiques (ECC) est une technique à clés publiques qui existe depuis 1986 mais dont la popularité est toute récente. Une courbe elliptique est un object mathématique abstrait possédant des propriétés algébriques fort intéressantes. En exploitant ces propriétés et la difficulté de certains problèmes mathématiques sur les courbes elliptiques, on peut construire des algorithmes cryptographiques permettant de fournir des services de base comme la signature électronique, le cryptage et l'échange de clés.

La sécurité de ECC est basée sur la difficulté à résoudre le problème du logarithme discret. En général, ce problème requiert un effort de calculs de type exponentiel. Toutefois, il existe certaines courbes pour lesquelles le problème du logarithme discret est plus facile à résoudre. Il faut savoir reconnaître ces courbes et les éviter.

Les systèmes de cryptographie sur courbes elliptiques se comparent avantageusement aux systèmes à clés publiques classiques comme Rivest-Shamir-Adleman (RSA). En effet, ces derniers ne requierent en général que des efforts de calculs sous-exponentiels pour être brisés. Ainsi, les systèmes ECC offrent une meilleure sécurité par bit de clé. Ils sont aussi efficaces du point de vue de la vitesse d'exécution, de l'espace de stockage, etc. Mentionnons en particulier, que les systèmes ECC sont tout à fait désignés pour offrir des services cryptographiques dans des environnements restreints comme les téléphones portables, les téléavertisseurs et les cartes à puce.

La cryptographie sur courbes elliptiques fait maintenant partie de plusieurs normes internationales. Notons entre autres ISO/IEC, ANSI, SECG, IEEE, FIPS, RFC et PKCS. Ces normes vont aider à faire connaître cette technique et vont faciliter sa mise en application à l'échelle internationale.

J. Rostand, Courbes elliptiques et cryptographie. TM 2001-095, CRDO, 2001.

Executive Summary

Communications and electronic transactions are becoming more and more numerous, especially since the beginning of the commercial Internet era. Cryptography is essential for having efficient authentication systems and good data protection.

Elliptic curve cryptography (ECC) is a public key technique that exists since 1986 but whose popularity is quite new. An elliptic curve is an abstract mathematical object that possesses several interesting algebraic properties. By exploiting those properties and the difficulty of some mathematical problems over elliptic curves, it is possible to construct cryptographic algorithms that can deliver basic services such as electronic signature, encryption and key exchange.

The security of ECC is based on the difficulty of solving the discrete logarithm problem. In general, that problem requires exponential type computing power. However, there are specific curves on which the discrete logarithm problem is much easier to solve. One must be able to recognize those curves and avoid them.

Elliptic curve cryptosystems have clear advantages over classical public key cryptosystems such as Rivest-Shamir-Adleman (RSA). Indeed, the later requires only sub-exponential amount of computations to be broken. Hence, ECC cryptosystems offer a better security per key bit. They are also efficient from the point of view of execution speed, storage space, etc. Let us mention that ECC is well designed for offering cryptographic services in resource constrained devices such as cell phones, pagers, smart cards, or any other low processing power devices.

Elliptic curve cryptography is now part of several international standards, in particular ISO/IEC, ANSI, SECG, IEEE, FIPS, RFC and PKCS. Those standards will help to promote ECC and will facilitate world scale implementations.

J. Rostand, Courbes elliptiques et cryptographie, TM 2001-095, DREO, 2001

P517601.PDF [Page: 10 of 64]

Table des matières

Résumé i

Abstract i

Sommaire iii

Executive Summary iv

Liste des figures vii

Liste des tableaux viii

1 Introduction 1

2 Structures algébriques de base 2

2.1 Notions de base sur les groupes 2

2.2 Notions de base sur les corps 5

2.2.1 Les corps finis 6

2.2.2 Représentations de $\mathbb{F}_{p^n}$ 7

3 Courbes elliptiques 14

3.1 Approche générale 14

3.2 Équations de Weierstrass 16

3.3 Structure de groupe 20

3.3.1 Courbe elliptiques sur $\mathbb{R}$ 20

3.3.2 Courbes elliptiques sur $\mathbb{F}_{p^n}$ $(p > 3)$ 22

3.3.3 Courbes elliptiques sur $\mathbb{F}_{2^n}$ et $\mathbb{F}_{3^n}$ 24

P517601.PDF [Page: 11 of 64]

4 Problème du logarithme discret **26**

4.1 Définition 26

4.2 Groupes d'intérêt en cryptographie 26

4.3 Comparaison entre différents PLD 27

5 Protocoles cryptographiques **29**

5.1 Elliptic Curve Digital Signature Algorithm (ECDSA) 29

5.2 Elliptic Curve Integrated Encryption Scheme (ECIES) 31

5.3 Elliptic Curve Diffie-Hellman Scheme (ECDHS) 33

6 Courbes elliptiques particulières **35**

6.1 Courbes elliptiques super-singulières 35

6.2 Courbes elliptiques anormales sur $\mathbf{Z}_p$ 36

6.3 Courbes elliptiques sur un sous-corps 36

6.4 Courbes elliptiques sur $\mathbf{F}_{2^m}$ où m est composé 36

6.5 Algorithme de Pohlig-Hellman 37

7 Normes régissant les SCCE **38**

7.1 Normes principales 39

7.2 Normes secondaires 41

8 Conclusion **44**

Références **45**

Liste des abréviations, acronymes et sigles **47**

P517601.PDF [Page: 12 of 64]

Liste des figures

1 Représentation d'une courbe elliptique dans $\mathbb{R}^3$ 16

2 Représentation cartésienne d'une courbe elliptique 18

3 Addition sur une courbe elliptique 21

P517601.PDF [Page: 13 of 64]

Liste des tableaux

1 Addition de points sur une courbe elliptique sur $\mathbb{R}$ 23

2 Addition de points sur une courbe elliptique sur $\mathbb{F}_{2^N}$ 23

1 Introduction

Les schémas de cryptage à clés publiques largement utilisés aujourd'hui sont basés pour la plupart sur des notions d'algèbre abstraite comme les groupes et les corps. Par exemple, Rivest-Shamir-Adleman (RSA), Diffie-Hellman, ElGamal et le *Digital Signature Algorithm* (DSA) sont différentes techniques cryptographiques qui utilisent d'une manière ou d'une autre la théorie des groupes. La sécurité de ces techniques est basée sur la difficulté à résoudre certains problèmes de la théorie des groupes. Par exemple, RSA est basé sur le fait qu'il est difficile de factoriser le produit n de deux premiers p et q lorsque ceux-ci sont suffisamment grands. En termes de la théorie des groupes, ce problème est celui de déterminer l'ordre du groupe $\mathbb{Z}_n^*$. Pour le protocole d'échange de clés Diffie-Hellman, le problème sous-jacent est celui du logarithme discret dans $\mathbb{Z}_p^*$

L'intérêt des courbes elliptiques en cryptographie est que celles-ci définissent naturellement des groupes. Ces derniers peuvent alors être utilisés dans des primitives cryptographiques. Il s'avère que sous certaines conditions, le problème du logarithme discret (PLD) dans un groupe associé à une courbe elliptique est plus difficile à résoudre que celui dans $\mathbb{Z}_p^*$ Ce qu'on veut dire par là, c'est que les meilleurs algorithmes connus pour résoudre le PLD dans le groupe d'une courbe elliptique sont moins efficaces que ceux spécialisés à $\mathbb{Z}_p^*$. Ainsi, dans les systèmes cryptographiques sur courbes elliptiques (SCCE), la sécurité par bit de clé est supérieure à celle des systèmes classiques. Cette raison, entre autres, a motivé la recherche dans ce secteur et les SCCE sont aujourd'hui de plus en plus présents dans les échanges électroniques

Le but de ce texte est de décrire comment les courbes elliptiques sont utilisées en général en cryptographie. Pour ce faire, nous aurons d'abord besoin de rappeler des notions de base d'algèbre, ce qui fait l'objet de la section suivante Ensuite, nous discuterons des courbes elliptiques en tant qu'objet mathématique et nous verrons comment celles-ci donnent lieu a des groupes. À la section 4, nous aborderons le problème du logarithme discret qui est à la base de toute la sécurité des SCCE Nous verrons à la section 5, comment on peut construire des protocoles cryptographiques d'encryption, de signature et d'échange de clés basés sur le PLD La sécurité des SCCE fera l'objet de la section 6. Nous terminerons finalement notre étude en brossant le tableau des différentes normes internationales dans lesquelles les SCCE sont traités et impliqués

2 Structures algébriques de base

Dans ce texte, deux structures algébriques retiendront particulièrement notre attention Il s'agit des groupes et des corps Ces structures sont fondamentales en algèbre et apparaissent constamment en cryptographie. Les notions présentées ici se retrouvent dans tous les livres de base en algèbre et structures algébriques. Le lecteur intéressé à en savoir davantage peut consulter par exemples les livres de Herstein [1] et Hungerford [2].

2.1 Notions de base sur les groupes

Les groupes sont des objets mathématiques à la fois simples et riches Ils sont faciles à définir mais sont aussi nombreux et ont des propriétés fort diversifiées. Parmi les groupes élémentaires bien connus, notons les nombres entiers, les nombres réels, les matrices, les permutations, les rotations et réflexions, les polynômes, etc...

DÉFINITION 2 1 Un *groupe* est la donnée d'un ensemble G et d'une opération $\cdot$ qui associe à chaque paire d'éléments $x, y \in G$ un nouvel élément $x \cdot y \in G$ tel que les propriétés suivantes sont satisfaites

- **Associativité.** Pour chaque $x, y, z \in G$, on a $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- **Identité.** Il existe un élément de G noté 1 qui est tel que $1 \cdot x = x \cdot 1 = x$ pour chaque $x \in G$
- **Inverse.** Pour chaque élément $x \in G$ il existe un élément noté x^{-1} qui est tel que $x^{-1} \cdot x = x \cdot x^{-1} = 1$

Si de plus la propriété suivante est satisfaite, on dit que G est un *groupe commutatif* ou encore un *groupe abélien*

- **Commutativité.** Pour chaque $x, y \in G$, on a $x \cdot y = y \cdot x$

NOTATION On écrit parfois $\langle G, \cdot \rangle$ pour représenter le groupe G muni de l'opération $\cdot$ Cela permet d'éviter certaines confusions lorsqu'un même ensemble est doté de plusieurs opérations

- **Groupe multiplicatif.** On dit d'un groupe qu'il est multiplicatif (en raison du symbole $\cdot$ rappelant la multiplication habituelle) si la notation précédente est utilisée. Dans cette notation le produit d'un élément x par lui même est noté x^n, où n est un entier Par exemple

$$x^2 = x \cdot x, \quad x^3 = x \cdot x \cdot x, \quad x^{-2} = x^{-1} \cdot x^{-1}, \quad x^{-3} = x^{-1} \cdot x^{-1} \cdot x^{-1}.$$

- **Groupe additif.** Il est aussi commun d'utiliser le symbole $+$ (au lieu de $\cdot$) pour représenter l'opération du groupe. On dit alors que le groupe est additif. On note l'élément identité par 0 et l'élément inverse de x par $-x$. De même, la somme d'un élément avec lui même est noté nx ($n \in \mathbb{Z}$).

$$2x = x + x, \quad 3x = x + x + x. \quad (-2)x = (-x) + (-x), \quad \text{etc}$$

  Notons que la notation additive est normalement réservée aux groupes commutatifs.

La notation choisie (additive ou multiplicative) pour décrire un groupe n'a évidemment aucune influence sur les propriétés de celui-ci. Il faut cependant porter une attention particulière au style de notation lorsque qu'un même ensemble est muni de deux opérations distinctes.

Voici quelques exemples classiques de groupes.

EXEMPLE 2.1 Soit $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ et soit $\cdot$ l'opération de multiplication habituelle sur les nombres réels. Alors $\langle \mathbb{R}^*, \cdot \rangle$ est un groupe commutatif (notation multiplicative). Dans ce groupe $3 \cdot 4 = 12$, $1 \cdot 5 = 5$ et $7^{-1} = 1/7$. □

EXEMPLE 2.2 L'ensemble des entiers muni de la somme habituelle $\langle \mathbb{Z}, + \rangle$ est un groupe commutatif (notation additive). L'identité est le nombre entier 0. On a $(-2)+5 = 3$, $-(5) = (-5)$ et $3 + 0 = 3$. □

EXEMPLE 2.3 Soit $\mathbb{Z}_n := \{0, \ldots, n-1\}$ et $+$ l'opération d'addition modulo n (la somme de deux entiers x et y modulo n est le reste de la division de $x + y$ par n, donc un nombre entier entre 0 et $n-1$ inclusivement). Alors $\langle \mathbb{Z}_n, + \rangle$ est un groupe abélien. Son identité est 0. Quelques exemples d'égalités dans $\mathbb{Z}_5$: $3 + 4 = 2$, $-4 = 1$, $8(2) = 1$.

EXEMPLE 2.4 Si on note par $\cdot$ l'opération multiplication modulo n, alors $\langle \mathbb{Z}_n^*, \cdot \rangle$ est un groupe où $\mathbb{Z}_n^* := \{k \in \mathbb{N} : \ 1 \leq k < n, \ \text{pgcd}(k, n) = 1\}$. Par exemple, $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ et dans $\mathbb{Z}_9^*$, on a $2 \cdot 7 = 5$, $5^2 = 7$ et $8 \cdot 4 = 5$. □

EXEMPLE 2.5 $\langle \mathbb{Z}_n \setminus \{0\}, \cdot \rangle$ n'est pas un groupe si n n'est pas premier. Par exemple dans $\mathbb{Z}_6 \setminus \{0\}$, le produit de 2 par 3 donne un élément qui n'est pas dans $\mathbb{Z}_6 \setminus \{0\}$ (il faudrait que ce soit 0). $\langle \mathbb{Z}_6, \cdot \rangle$ n'est pas non plus un groupe puisque 0 ne possède pas d'inverse. □

EXEMPLE 2.6 Soit $M_n^{-1}(\mathbb{C})$ l'ensemble des matrices $n \times n$ inversibles à coefficients complexes et soit $\cdot$ le produit matriciel habituel. Alors $\langle M_n^{-1}(\mathbf{C}), \cdot \rangle$ est un groupe non

P517601.PDF [Page: 17 of 64]

commutatif □

EXEMPLE 2 7 Soit X un ensemble fini et soit P_X l'ensemble des permutations de X. Alors $\langle P_X, \circ \rangle$ est un groupe, où $\circ$ est l'opération de composition □

Les groupes sont des structures mathématiques très riches Il existe tout un vocabulaire pour décrire leurs différentes propriétés. Les termes suivants sont couramment utilisés

DÉFINITION 2 2 Soit $\langle G, \cdot \rangle$ un groupe

- *L'ordre du groupe* G, noté $|G|$ est le nombre d'éléments de G
- Le groupe G est dit *fini* si $|G| < \infty$
- *L'ordre d'un élément* x de G est le plus petit entier $n \geq 1$ tel que $x^n = 1$ Si un tel entier n'existe pas, on dit alors que x est d'ordre infini
- Un sous-ensemble H de G est un *sous-groupe* de G si $\langle H, \cdot \rangle$ est un groupe
- Soit $x \in G$. L'ensemble $\langle x \rangle := \{x^n \ . \ n \in \mathbb{Z}\} \subset G$ est un sous-groupe de G. On dit que $\langle x \rangle$ est le *sous-groupe de* G *engendré par* x.
- Le groupe G est *cyclique* s'il existe un élément $x \in G$ tel que $\langle x \rangle = G$. On dit alors que x est un *générateur* de G.

EXEMPLE 2 8 L'ordre du groupe multiplicatif $\mathbb{Z}_{28}^*$ est $\phi(28) = 12$ (où $\phi(n)$ est la fonction d'Euler comptant le nombre d'entier inférieur à n et relativement premier à n) En effet,

$$\mathbb{Z}_{28}^* = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}.$$

L'ordre de l'élément 5 est 6 puisque $5^6 \equiv 1 \mod 28$ et que $5^k \not\equiv 1 \mod 28$ pour $k = 1, \ldots, 5$ Le sous-groupe de $\mathbb{Z}_{28}^*$ engendré par 3 est $H := \langle 3 \rangle = \{1, 3, 9, 19, 25, 27\}$. Il s'agit d'un groupe cyclique (mais $\mathbb{Z}_{28}^*$ n'est pas cyclique, comme on peut le vérifier) L'élément 19 est aussi un générateur de H. □

Nous utiliserons, dans la suite, la proposition suivante

PROPOSITION 2 1

1) Si H est un sous-groupe d'un groupe fini G, alors $|H|$ divise $|G|$
2) L'ordre d'un élément x d'un groupe fini G est un diviseur de $|G|$.

Le dernier enoncé est déduit du premier en considérant le sous-groupe $H := \langle x \rangle$

2.2 Notions de base sur les corps

Passons maintenant à la notion de corps. Un corps est un ensemble qui possède deux structures de groupe distinctes : une structure additive et une structure multiplicative. L'ensemble des nombres réels muni de l'addition et de la multiplication habituelles forme un corps. Dans un corps, on peut faire les opérations d'addition, soustraction, multiplication et division (sauf par zéro pour cette dernière). Voici la définition algébrique d'un corps.

DÉFINITION 2.3 Un *corps* (commutatif) est la donnée d'un ensemble F et de deux opérations $+$ et $\cdot$ qui associent à chaque paire d'éléments $x, y \in F$ deux nouveaux éléments de F, leur somme $x + y$ et leur produit $x \cdot y$. De plus, les propriétés suivantes doivent être satisfaites :

- **Structure additive.** $\langle F, + \rangle$ est un groupe commutatif. Son identité est notée 0 et l'inverse (additif) d'un élément x est noté $-x$.
- **Structure multiplicative.** $\langle F^*, \cdot \rangle$ est un groupe commutatif. Ici, $F^* := F \backslash \{0\}$. L'identité de ce groupe est notée 1 et l'inverse (multiplicatif) d'un élément x est noté x^{-1}.
- **Distributivité.** Pour tout $x, y, z \in F$, on a $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

On écrit $\langle F, +, \cdot \rangle$ pour représenter le corps F muni des opérations $+$ et $\cdot$. Aussi, on réfère au groupe multiplicatif de F par la notation F^*.

EXEMPLE 2.9 L'ensemble des nombres réels $\mathbb{R}$ muni des opérations habituelles d'addition et de multiplication est un corps. □

EXEMPLE 2.10 De même, les nombres complexes $\mathbb{C}$ et les opérations habituelles d'addition et de multiplication sur ceux-ci forment un corps. □

EXEMPLE 2.11 L'ensemble $\mathbb{Z}_p := \{0, 1, \ldots, p-1\}$ muni des opérations d'addition et de multiplication modulo p est un corps si et seulement si p est premier. □

Voici maintenant en rafale quelques définitions de base concernant les corps. Ces termes sont couramment utilisés.

DÉFINITION 2.4 Soit $\langle F, +, \cdot \rangle$ un corps.

- *L'ordre d'un corps* F, noté $|F|$ est le nombre d'éléments de F.
- Le corps F est dit *fini* si $|F| < \infty$.

- La *caractéristique d'un corps* F est le plus petit entier n tel que $\sum_{k=1}^{n} 1 = 0$ Si un tel entier n n'existe pas, on dit que F est de caractéristique 0

- Un sous-ensemble E de F est un *sous-corps* de F si $\langle E, +, \cdot \rangle$ est un corps On dit alors que F est un *corps d'extension* ou simplement une *extension* de E

EXEMPLE 2 12 Les corps $\mathbb{R}$ et $\mathbb{C}$ sont infinis et de caractéristique 0. Le corps $\mathbb{R}$ est un sous-corps de $\mathbb{C}$ (en considérant que les nombres réels sont des nombres complexes dont la partie imaginaire est nulle) et donc, $\mathbb{C}$ est un corps d'extension de $\mathbb{R}$ Le corps $\mathbb{Z}_p$ (p un nombre premier) est fini, son ordre est p et sa caractéristique est p. Pour deux premiers distincts p_1 et p_2, $\mathbb{Z}_{p_1}$ n'est jamais un sous-corps de $\mathbb{Z}_{p_2}$. □

Prenant pour acquis les notions de base sur les espaces vectoriels, on peut relier la notion de sous-corps et d'espace vectoriel de la manière suivante.

PROPOSITION 2 2 Soit E un sous-corps de F Alors F est un espace vectoriel sur E. L'addition et la multiplication par un scalaire sont simplement les opérations de F La dimension de cet espace vectoriel est notée $[F : E]$ et est appelée le *degré de F sur E*

2.2.1 Les corps finis

Les corps finis jouent un rôle important en cryptographie et du fait même, ils méritent une attention particulière. Voici quelques résultats classiques sur les corps finis

PROPOSITION 2 3

1) Si F est un corps fini, alors $|F| = p^n$ pour un certain premier p et un certain entier $n \geq 1$

2) Pour chaque entier $n \geq 1$ et chaque premier p, il existe un unique corps d'ordre p^n (à un isomorphisme près) Ce corps est dénoté $\mathbb{F}_{p^n}$ ou encore $\mathrm{GF}(p^n)$

REMARQUE 2 1 Un isomorphisme entre deux corps F et G est une bijection ϕ entre F et G telle que $\phi(x + y) = \phi(x) + \phi(y)$ et $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ pour chaque paire $(x, y) \in F \times F$ Lorsqu'un isomorphisme existe entre deux corps, ceux-ci ont le même nombre d'éléments et possèdent la même structure algébrique Il sont identiques du point de vue algébrique.

En conséquence de la proposition précédente, tous les corps d'ordre p sont structurellement identiques au corps $\mathbb{Z}_p$ Ils seront notés indifféremment par $\mathbb{F}_p$ ou $\mathbb{Z}_p$ Nous verrons

dans quelques instant comment construire une représentation des corps d'ordre p^n pour $n \geq 2$. Mais juste auparavant, voyons quelques faits concernant les corps finis.

PROPOSITION 2 4 Soient p un premier, n un entier positif non nul et q une puissance d'un nombre premier. Les énoncés suivants sont vrais

1) La caractéristique du corps $\mathbb{F}_{p^n}$ est p

2) $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q-1$ et donc $a^q = a$ pour chaque $a \in \mathbb{F}_q$. Un générateur de $\mathbb{F}_q^*$ est appelé un *élément primitif* ou un *générateur* de $\mathbb{F}_q$.

3) Un élément $a \in \mathbb{F}_{p^n}$ est dans le sous-corps $\mathbb{F}_{p^d}$ si et seulement si $a^{p^d} = a$.

4) $\mathbb{F}_q$ est un sous-corps de $\mathbb{F}_{p^n}$ si et seulement si $q = p^d$ où d divise n. En particulier, $\mathbb{F}_p = \mathbb{Z}_p$ est toujours un sous-corps de $\mathbb{F}_{p^n}$.

5) Pour chaque $t \in \mathbb{Z}$ et chaque $a, b \in \mathbb{F}_{p^n}$ on a

$$(a+b)^{p^t} = a^{p^t} + b^{p^t}.$$

2.2.2 Représentations de $\mathbb{F}_{p^n}$

Puisque $\mathbb{F}_p$ est un sous-corps de $\mathbb{F}_{p^n}$, ce dernier est un espace vectoriel sur $\mathbb{F}_p$. Cet espace vectoriel est de dimension $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Donc, pour chaque corps $\mathbb{F}_{p^n}$ il existe une base $\{e_1, \ldots, e_n\}$ d'éléments de $\mathbb{F}_{p^n}$ telle que chaque élément $a \in \mathbb{F}_{p^n}$ peut être représenté de manière unique sous la forme

$$a = a_1 e_1 + \cdots a_n e_n,$$

où $a_i \in \{0, \ldots p-1\} = \mathbb{F}_p = \mathbb{Z}_p$ et $i \in \{1, \ldots, n\}$.

Lorsque $p = 2$, on dit que $\mathbb{F}_{2^n}$ est un *corps fini binaire*. Dans ce cas particulier important en cryptographie, les coefficients a_i prennent les valeurs 0 ou 1 et la somme de deux éléments $a := \sum a_i e_i$ et $b := \sum b_i e_i$ se fait simplement par le OU exclusif (XOR) des deux vecteurs $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_n)$. La multiplication, elle, est dépendante de la base choisie. Théoriquement est vaut

$$a \cdot b = \sum_{i,j=1}^{n} a_i b_j e_i e_j.$$

ce qui implique le calcul des éléments $e_i e_j$ dans la base $\{e_1, \ldots, e_n\}$

Le choix de cette base devient donc relativement important lorsqu'il s'agit d'optimiser les performances de calculs. Nous allons regarder deux types particuliers de bases : les bases polynomiales et les bases normales. Le premier offre de meilleurs avantages dans les implémentations logicielles alors que le second est davantage performant dans les implémentations matérielles.

Bases polynomiales

Chaque polynôme irréductible de degré n sur $\mathbb{Z}_p$ définit une représentation à base polynomiale de $\mathbb{F}_{p^n}$. Supposons que

$$f(x) := x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0 \qquad (f_i \in \mathbb{Z}_p)$$

est un polynôme irréductible sur $\mathbb{Z}_p$, c'est-à-dire que les seuls diviseurs de $f(x)$ sont des polynômes de degrés 1 et n. On définit

$$F := \left\{ a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in \mathbb{Z}_p \right\}.$$

Muni des opérations d'addition et de multiplication qui suivent, F est un corps d'ordre p^n et donc, par des remarques faites précédemment, F est isomorphe à $\mathbb{F}_{p^n}$ et peut donc être utilisé comme une représentation de ce dernier.

- *Addition* La somme de deux éléments a et b de $\mathbb{F}_{p^n}$ est définie par la somme habituelle de polynômes. La somme des coefficients s'effectue dans $\mathbb{Z}_p$.
- *Multiplication* Le produit de deux éléments a et b de $\mathbb{F}_{p^n}$ est le reste de la division par $f(x)$ du produit habituel des polynômes a et b. Cette opération est parfois dénotée $ab \bmod f(x)$. Évidemment l'arithmétique des coefficients se fait toujours dans $\mathbb{Z}_p$.

Les éléments de $\mathbb{F}_{p^n}$ sont parfois représentés sous forme de vecteur, ce qui rend la notation plus compacte.

$$(a_{n-1}, a_{n-2}, \ldots, a_1, a_0) := (a_{n-1}a_{n-2}\ldots a_1 a_0) := a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

EXEMPLE 2.13 Le polynôme $f(x) = x^4 + x + 1$ est irréductible sur $\mathbb{Z}_2$. En effet, $f(0) = f(1) = 1$ et donc f ne possède pas de zéro dans $\mathbb{Z}_2$. En conséquence aucun facteur linéaire ne divise $f(x)$. On vérifie facilement (4 cas) que le produit de deux polynômes quadratiques à coefficients dans $\mathbb{Z}_2$ ne donne jamais $f(x)$. Ainsi, on peut représenter les $2^4 = 16$ éléments de $\mathbb{F}_{2^4}$ par les polynômes suivants :

0	x^2	x^3	$x^3 + x^2$
1	$x^2 + 1$	$x^3 + 1$	$x^3 + x^2 + 1$
x	$x^2 + x$	$x^3 + x$	$x^3 + x^2 + x$
$x + 1$	$x^2 + x + 1$	$x^3 + x + 1$	$x^3 + x^2 + x + 1$.

ou sous forme abrégée

$$\begin{array}{cccc} (0000) & (0100) & (1000) & (1100) \\ (0001) & (0101) & (1001) & (1101) \\ (0010) & (0110) & (1010) & (1110) \\ (0011) & (0111) & (1011) & (1111). \end{array}$$

Pour illustrer les opérations d'addition et de multiplication, prenons les éléments $a := x^2 + x = (0110)$ et $b := x^3 + x^2 + x + 1 = (1111)$ de $\mathbb{F}_{2^4}$. Alors

$$\begin{aligned} a + b &= (x^2 + x) + (x^3 + x^2 + x + 1) \\ &= x^3 + (1+1)x^2 + (1+1)x + 1 \\ &= x^3 + 1 = (1001) \end{aligned}$$

Aussi,

$$\begin{aligned} ab &= (x^2 + x)(x^3 + x^2 + x + 1) \\ &= x^5 + (1+1)x^4 + (1+1)x^3 + (1+1)x^2 + x \\ &= x^5 + x. \end{aligned}$$

Or, en divisant $x^5 + x$ par $f(x)$, on trouve que $x^5 + x = x(x^4 + x + 1) - x^2$ et donc, $x^5 + x \equiv x^2 \bmod f(x)$. Ainsi,

$$ab = x^2 = (0100)$$

Ici, $\alpha := x = (0010)$ est un générateur de $\mathbb{F}_{2^4}$. Le calcul des puissances successives de x montre ce fait

$$\begin{array}{llllll} x^0 = 1 & & x^6 = x^3 + x^2 & & x^{12} = x^3 + x^2 + x + 1 \\ x^1 = x & & x^7 = x^3 + x + 1 & & x^{13} = x^3 + x^2 + 1 \\ x^2 = x^2 & & x^8 = x^2 + 1 & & x^{14} = x^3 + 1 \\ x^3 = x^3 & & x^9 = x^3 + x & & x^{15} = 1 \\ x^4 = x + 1 & & x^{10} = x^2 + x + 1 & & \\ x^5 = x^2 + x & & x^{11} = x^3 + x^2 + x & & \end{array}$$

□

Bases normales

Les bases normales constituent un autre choix pour la représentation des éléments d'un corps fini $\mathbb{F}_{p^n}$. Dans le cas des corps binaires ($p = 2$), l'opération $\alpha \mapsto \alpha^2$ devient simplement une rotation des coefficients de α dans la base normale. Cette particularité rend ce choix de base particulièrement intéressant pour les applications matérielles.

Une *base normale* pour $\mathbb{F}_{p^n}$ est une base de $\mathbb{F}_{p^n}$ de la forme

$$\left\{\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}\right\},$$

P517601.PDF [Page: 23 of 64]

où β est un élément de $\mathbb{F}_{p^n}$. Pour chaque corps fini, une telle base existe toujours (voir par exemple [3]) Ainsi, une fois β fixé, chaque élément a de $\mathbb{F}_{p^n}$ peut être uniquement représenté sous la forme

$$a = a_{n-1}\beta^{p^{n-1}} + \cdots + a_2\beta^{p^2} + a_1\beta^p + a_0\beta = \sum_{i=0}^{n-1} a_i\beta^{p^i}$$

où $a_i \in \mathbb{Z}_p$ $(i = 0, \ldots, n-1)$ Comme dans le cas des bases polynomiales, on utilise parfois une notation abrégée

$$a = (a_{n-1}a_{n-2}\ldots a_1a_0) = \sum_{i=0}^{n-1} a_i\beta^{p^i}.$$

Soit $\left\{\beta^{p^0}. \quad ., \beta^{p^{n-1}}\right\}$ une base normale pour $\mathbb{F}_{p^n}$ et soient $a = (a_{n-1}a_{n-2}\ldots a_1a_0)$ et $b = (b_{n-1}b_{n-2}. \ . b_1b_0)$ deux éléments de $\mathbb{F}_{p^n}$ exprimés dans cette base.

- *Addition*. La somme de a et b est

  $$\sum_{i=0}^{n-1} a_i\beta^{p^i} + \sum_{i=0}^{n-1} b_i\beta^{p^i} - \sum_{i=0}^{n-1} (a_i + b_i)\beta^{p^i},$$

  où la somme des coefficients s'effectue dans $\mathbb{Z}_p$.

- *Multiplication* Le produit de a et b est plus compliqué. Puisque $\mathbb{F}_{p^n}$ est un corps, on a

  $$c := ab = \left(\sum_{i=0}^{n-1} a_i\beta^{p^i}\right) \cdot \left(\sum_{i=0}^{n-1} b_i\beta^{p^i}\right) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_ib_j\beta^{p^i}\beta^{p^j}.$$

  D'autre part, dans la base normale engendrée par β, l'élément c possède la représentation

  $$c = \sum_{k=0}^{n-1} c_k\beta^{p^k},$$

  pour certains $c_k \in \mathbb{Z}_p$ $(k = 0, \ldots, n-1)$. Il faut donc résoudre les équations précédentes pour ces inconnues c_k.

Puisque chaque produit $\beta^{p^i}\beta^{p^j}$ est un élément de $\mathbb{F}_{p^n}$, il peut être représenté dans la base normale. Notons par $\lambda_{ij}^{(k)}$ les éléments de $\mathbb{Z}_p$ tels que pour chaque i et chaque j on a

$$\beta^{p^i}\beta^{p^j} = \sum_{k=0}^{n-1} \lambda_{ij}^{(k)}\beta^{p^k}. \tag{1}$$

Les matrices $\Lambda_k := (\lambda_{ij}^{(k)})$ sont appelées les *tables de multiplication* de la base normale. Lorsque ces tables sont connues, on calcule $c := ab$ comme suit

$$c = \sum_{k=0}^{n-1} c_k\beta^{p^k} = \sum_{k=0}^{n-1} \left(\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_ib_j\lambda_{ij}^{(k)}\right)\beta^{p^k} = \sum_{k=0}^{n-1} a\Lambda_k b^t\beta^{p^k},$$

où l'expression $a\Lambda_k b^t$ est interprétée comme un produit matriciel dans lequel a et b sont des matrices $1 \times n$ et où b^t est la transposée de b

Un fait intéressant des bases normales est que leurs tables Λ_k ne sont pas indépendantes En effet, on peut, pour chaque k, exprimer Λ_k en termes de Λ_0 Fixons un entier l et prenons la puissance p^{-l} de chaque membre de l'équation (1). On trouve

$$\beta^{p^{i-l}}\beta^{p^{j-l}} = \left(\sum_{k=0}^{n-1}\lambda_{ij}^{(k)}\beta^{p^k}\right)^{p^{-l}} = \sum_{k=0}^{n-1}\left(\lambda_{ij}^{(k)}\right)^{p^{-l}}\beta^{p^{k-l}},$$

où on a utilisé la proposition 2 4-3 Chaque exposant de p dans l'équation précédente peut être considéré modulo n puisque $\alpha^{p^n} = 1$ pour chaque $\alpha \in \mathbb{F}_{p^n}$ (voir proposition 2.4-2) En utilisant à nouveau l'équation (1) pour le membre de gauche et la proposition 2.4-3 pour le membre de droite, on trouve

$$\sum_{k=0}^{n-1}\lambda_{i-l,j-l}^{(k)}\beta^{p^k} = \sum_{k=0}^{n-1}\lambda_{ij}^{(k)}\beta^{p^{k-l}}.$$

En égalant les coefficients de β de chaque membre, on a

$$\lambda_{i-l,j-l}^{(0)} = \lambda_{ij}^{(l)}.$$

Ainsi, la matrice Λ_l est obtenue de Λ_0 par une rotation des lignes et des colonnes de cette dernière. Notons simplement par Λ la matrice Λ_0

La multiplication de a et b est donc donnée par

$$c = \sum_{k=0}^{n-1}\left(\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}a_i b_j \lambda_{i-k,j-k}\right)\beta^{p^k}.$$

EXEMPLE 2 14 Considérons le corps $\mathbb{F}_{2^4}$ de la section précédente et posons $\beta := x^3$ Alors l'ensemble $\left\{\beta, \beta^2, \beta^{2^2}, \beta^{2^3}\right\}$ forme une base normale pour $\mathbb{F}_{2^4}$. Les éléments $a := x^3 + x^2 + x$ et $b := x$ dans la représentation polynomiale modulo $f(x) = x^4 + x + 1$, s'écrivent maintenant

$$a = \beta^{2^3} + \beta = (1011) \quad \text{et} \quad b = \beta^{2^3} + \beta^{2^1} + \beta = (1001).$$

Leur somme $a + b$ est (0100). La table de multiplication Λ associée à la base normale $\left\{\beta, \beta^2, \beta^{2^2}, \beta^{2^3}\right\}$ est

$$\Lambda = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Le produit de a et b est donc

$$\begin{aligned} ab &= \sum_{k=0}^{3} \left(\sum_{i=0}^{3} \sum_{j=0}^{3} a_i b_j \lambda_{i-k,j-k} \right) \beta^{p^k} \\ &= \sum_{k=0}^{3} \left(\sum_{i=0}^{3} a_i (\lambda_{i-k,-k} + \lambda_{i-k,3-k}) \right) \beta^{p^k} \\ &= \sum_{k=0}^{3} (\lambda_{-k,-k} + \lambda_{-k,3-k} + \lambda_{1-k,-k} + \lambda_{1-k,3-k} + \lambda_{3-k,-k} + \lambda_{3-k,3-k}) \beta^{p^k} \\ &= (1+1, 1+1+1+1, 1+1, 1+1) \\ &= (0100). \end{aligned}$$

□

Une des particularités des bases normales sur $\mathbb{F}_{2^n}$ est que le carré d'un élément $a = (a_{n-1}a_{n-2}\cdots a_1 a_0)$ est simplement $a^2 = (a_{n-2}a_{n-3}\cdots a_0 a_{n-1})$. Ce fait est particulièrement intéressant pour des calculs explicites de puissances, lorsqu'on utilise la technique *square and multiply* L'opération de mise au carré est très performante puisqu'elle ne consiste qu'à faire un décalage des coefficients (bits) de l'argument.

EXEMPLE 2 15 Dans le contexte de l'exemple précédent, on peut calculer a^9 de la manière suivante.

$$a^9 = a\left(\left(a^2\right)^2\right)^2 = (1011)\left((0111)^2\right)^2 = (1011)(1110)^2 = (1011)(1101) = (1000).$$

La dernière égalité est obtenue en appliquant la table de multiplication Λ □

Bases normales optimales

Pour que les bases normales soient utiles en pratique, il faut que l'opération de multiplication ne soit pas trop coûteuse La clé est la table de multiplication Λ définie ci-haut. Plus il y a de 0 dans cette table, moins il est nécessaire d'effectuer des opérations dans $\mathbb{Z}_p$ pour calculer le produit de deux éléments de $\mathbb{F}_{p^n}$.

Le nombre d'entrées non nulles de la matrice de multiplication Λ d'une base normale N est appelé *la complexité de* N et est noté c_N. On peut montrer (voir [4, 5]) que pour toute base normale N de $\mathbb{F}_{p^n}$, on a $c_N \geq 2n-1$. Une base normale est dite *optimale* lorsque $c_N = 2n-1$

Un corps fini $\mathbb{F}_{p^n}$ possède toujours une base normale, mais pas toujours une base normale optimale On connaît toutefois des critères permettant de vérifier si un corps donné possède une base normale optimale et, le cas échéant, une méthode pour la construire

(voir [6, Chapter 4]) On distingue deux types de bases normales optimales : les types I et II. Ceux-ci réfèrent à la méthode de construction utilisée.

Pour des constructions concrètes de bases normales optimales dans $\mathbf{F}_{2^n}$ (le cas d'intérêt en cryptographie), le lecteur peut consulter le chapitre 4 de [7]

3 Courbes elliptiques

La sécurité des protocoles cryptographiques comme Diffie-Hellman et ElGamal est basée sur le problème du logarithme discret dans le groupe cyclique $\mathbb{Z}_p^*$. Ces protocoles peuvent être transportés dans d'autres groupes. L'intérêt des courbes elliptiques en cryptographie vient du fait qu'à chacune de celles-ci est naturellement associé un groupe. Les techniques spécialisées pour résoudre le problème du logarithme discret dans $\mathbb{F}_q^*$ semblent ne pas s'adapter directement au cas des courbes elliptiques. Ainsi, en ce moment, seuls des algorithmes généraux (pouvant s'appliquer à tous les groupes) peuvent être utilisés pour résoudre le problème du logarithme discret sur des courbes elliptiques. Ces algorithmes ont des temps d'exécution exponentiels ce qui les rend moins performant que ceux spécialisés aux groupes $\mathbb{F}_q^*$, ces derniers étant sous-exponentiels. Par conséquence la sécurité des protocoles basés sur les courbes elliptiques est plus grande pour une même longueur de clé que ceux basés sur les groupes $\mathbb{Z}_p^*$.

Dans cette section, nous allons définir la notion de courbes elliptiques. Une courbe elliptique est un ensemble de points satisfaisant une relation d'un certain type. Nous verrons d'abord des courbes elliptiques générales définies sur un corps K. Puis nous parlerons de la classification des courbes elliptiques, ce qui nous mènera aux équations de Weierstrass. Finalement, pour chaque courbe elliptique, nous verrons comment il est possible de définir une structure de groupe. C'est cette dernière qui est sollicitée en cryptographie.

3.1 Approche générale

Avant de définir proprement dit les courbes elliptiques, il faut se munir de quelques outils de géométrie algébrique.

DÉFINITION 3.1 Soit K un corps et soit $\sim$ la relation d'équivalence sur K^3 définie par

$$(X_0, Y_0, Z_0) \sim (X_1, Y_1, Z_1) \iff \exists k \in K^* \text{ t.q. } (X_0, Y_0, Z_0) = k(X_1, Y_1, Z_1).$$

Le *plan projectif* $\mathbb{P}^2(K)$ associé à K est le quotient de $K^3 \setminus \{(0,0,0)\}$ par $\sim$

$$\mathbb{P}^2(K) := \frac{K^3 \setminus \{(0,0,0)\}}{\sim}.$$

Deux points de $K^3 \setminus \{(0,0,0)\}$ sur une même droite passant par l'origine sont considérés identiques dans $\mathbb{P}^2(K)$. Dans le cas $K = \mathbb{R}$, on peut voir $\mathbb{P}^2(\mathbb{R})$ comme étant la sphère unité de $\mathbb{R}^3$ dont les points diamétralement opposés sont identifiés. Un triplet (X, Y, Z) d'une classe d'équivalence d'un point P de $\mathbb{P}^2(K)$ est appelé les *coordonnées homogènes* de P.

NOTATION Soit K un corps. On note par $K[x]$ l'ensemble des polynômes à coefficients dans K dont la variable est x. Autrement dit,

$$K[x] := \left\{ \sum_{i=0}^{n} k_i x^i : k_i \in K,\ n = 0, 1, \ldots \right\}.$$

Pour les polynômes en plusieurs variables, on utilise la notation $K[x_1, \ldots, x_N]$. Ainsi, par exemple,

$$K[X, Y, Z] := \left\{ \sum_{i,j,k \geq 0} k_{ijk} X^i Y^j Z^k : k_{ijk} \in K \right\},$$

où les sommes $\sum_{i,j,k}$ sont finies.

DÉFINITION 3 2 Une *courbe* de $\mathbb{P}^2(K)$ est l'ensemble solution d'une équation de la forme

$$p(X, Y, Z) = 0$$

où $p \in K[X, Y, Z]$ est un polynôme homogène de degré d.

Par exemple, l'équation

$$X^2 Y + X Z^2 + 3XYZ = 0$$

définit une courbe cubique ($d = 3$) de $\mathbb{P}^2(\mathbb{Z}_5)$.

DÉFINITION 3 3 Une courbe $C : p(X, Y, Z) = 0$ de $\mathbb{P}^2(K)$ est dite *non singulière* si en chacun de ses points elle admet une tangente. On peut montrer que cette condition est équivalente à

$$\nabla p(X, Y, Z) := \left(\frac{\partial p}{\partial X}(X, Y, Z), \frac{\partial p}{\partial Y}(X, Y, Z), \frac{\partial p}{\partial Z}(X, Y, Z) \right) \neq (0, 0, 0)$$

en chaque point $(X, Y, Z) \in C$. À noter que les dérivées peuvent être définies de manière purement algébrique puisque p est un polynôme. On dit de la courbe qu'elle est *singulière* si elle n'est pas *non singulière*.

EXEMPLE 3 1 La courbe cubique $p_1 := X^3 + Y^3 + Z^3 = 0$ de $\mathbb{P}^2(K)$ est non singulière sur les corps K dont la caractéristique n'est pas 3, en effet, $\nabla p_1 = 3(X^2, Y^2, Z^2) \neq (0, 0, 0)$ pour chaque $(X, Y, Z) \in \mathbb{P}^2(K)$. À l'opposé, la courbe cubique $p_2 := X^2 Y + Z^3 = 0$ de $\mathbb{P}^2(K)$ est singulière (pour chaque corps K!) au point $P = (0, 1, 0)$ puisque $\nabla p_2(0, 1, 0) = (0, 0, 0)$. □

DÉFINITION 3 4 Une *courbe elliptique E sur un corps K* est une courbe cubique non singulière de $\mathbb{P}^2(K)$. On note par $E(K)$ l'ensemble des solutions de cette courbe cubique, c'est-à-dire l'ensemble des points de la courbe elliptique E.

EXEMPLE 3 2 La cubique $X^3 - 2XZ^2 + 2Z^3 - Y^2 Z = 0$ de $\mathbb{P}^2(\mathbb{R})$ est une courbe elliptique sur le corps $\mathbb{R}$. Un simple calcul montre que la courbe est non singulière. En

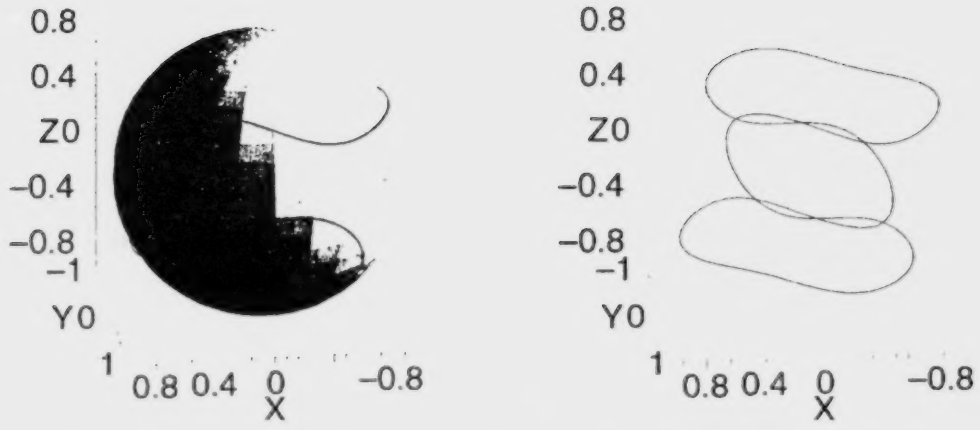

FIG 1 – Représentation de la courbe elliptique $X^3 - 2XZ^2 + 2Z^3 - Y^2Z = 0$.

effet, $\nabla p = (3X^2 - 2Z^2, -2YZ, -4XZ + 6Z^2 - Y^2) = (0,0,0)$ implique que $X = Y = Z = 0$, mais ce point n'est pas dans $\mathbb{P}^2(\mathbb{R})$ (par la définition du plan projectif). La représentation de $\mathbb{P}^2(\mathbb{R})$ par une sphère dans $\mathbb{R}^3$ nous permet de visualiser la courbe elliptique (voir la figure 1). Il faut cependant garder en mémoire que chaque point de la courbe est identifié à son symétrique par rapport à l'origine □

EXEMPLE 3.3 Considérons le corps $K = \mathbb{F}_{2^3}$ et le point $a = x^2 = (100) \in \mathbb{F}_{2^3}$ en représentation polynomiale modulo $f(x) = x^3 + x + 1$. On peut montrer que a est un générateur de $\mathbb{F}_{2^3}$. La cubique

$$Y^2Z + XYZ - X^3 - aX^2Z - Z^3 = 0$$

est non singulière. Il s'agit donc d'une courbe elliptique sur $\mathbb{F}_{2^3}$. En coordonnées homogènes, les points de cette courbes sont

$$E(K) := \left\{(0,1,0), (0,1,1), (a,1,a), (a^5,1,a^5)\right\}.$$

□

3.2 Équations de Weierstrass

DÉFINITION 3.5 Deux courbes elliptiques E et $\tilde{E}$ définies sur un même corps K sont dites *isomorphes* s'il existe un changement de variables rationnel ϕ qui transforme l'équation de E en celle de $\tilde{E}$. Cela veut dire que ϕ est une application bijective de $\mathbb{P}^2(K)$ sur lui-même qui est de la forme

$$\phi(X,Y,Z) := \left(\tilde{X}(X,Y,Z), \tilde{Y}(X,Y,Z), \tilde{Z}(X,Y,Z)\right)$$

où $\tilde{X}$, $\tilde{Y}$ et $\tilde{Z}$ sont des quotients de polynômes en X, Y et Z dont les coefficients sont dans la clôture algébrique [†] de K. L'inverse de ϕ est de la même forme.

Lorsque deux courbes elliptiques sont isomorphes, elles possèdent les mêmes propriétés géométriques et algébriques. Pour les applications cryptographiques (qui elles s'intéressent aux structures de groupes des courbes elliptiques) elles sont donc considérées identiques

Les *équations de Weierstrass* sont des formes particulières d'équations cubiques Le théorème suivant montre que toutes les courbes elliptiques peuvent s'écrire sous cette forme par le biais d'un isomorphisme Il suffira donc dans la suite d'étudier les courbes elliptiques données sous la forme de Weierstrass

THÉORÈME 3 1 Soit E une courbe elliptique sur un corps K et soit P un point de E Alors il existe un isomorphisme ϕ de E sur une courbe elliptique $\tilde{E}$ tel que $\phi(P) = (0,1,0)$ et tel que $\tilde{E}$ est de la forme

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_1XZ^2 + a_6Z^3$$

pour certains coefficients $a_1, \ldots, a_6 \in K$. Le point $(0,1,0)$ est noté $\mathcal{O}$

Les équations de Weierstrass possèdent une propriété intéressante qui simplifie les notations. En effet, les seules solutions avec $Z = 0$ sont des points de la forme $(0,\alpha,0)$, où $\alpha \in K \setminus \{0\}$ Évidemment, tous ces points ne correspondent en fait qu'au seul et même point de $\mathbb{P}^2(K)$, à savoir $\mathcal{O}$. Ainsi, cela suggère une écriture plus simple pour les courbes elliptiques sous la forme de Weierstrass Posons $x := X/Z$ et $y := Y/Z$ Alors, l'équation d'une courbe elliptique E peut s'écrire sous la forme

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_1x + a_6. \tag{2}$$

À noter que dans cette notation, les points de E sont les points de la forme $(x,y,1)$ avec x et y solutions de (2), plus le point à l'infini $\mathcal{O} = (0,1,0)$.

EXEMPLE 3 4 La courbe $X^3 - 2XZ^2 + 2Z^3 - Y^2Z = 0$ de la section précédente a comme équation de Weierstrass

$$y^2 = x^3 - 2x + 2.$$

Dans le plan cartésien, cette courbe possède la représentation illustrée à la figure 2.

Le point $\mathcal{O}$ est le seul de la courbe elliptique qui ne peut être représenté dans le plan. Comme nous le verrons plus loin, ce point agit comme s'il était situé infiniment haut

[†]Une extension K' d'un corps K est dite *algébrique* sur K si chaque élément de K' est un zéro d'un polynôme de $K[x]$ La *clôture algébrique* $\overline{K}$ d'un corps K est une extension algébrique de K dans laquelle chaque polyôme non constant $p \in \overline{K}[x]$ possède un zéro dans $\overline{K}$

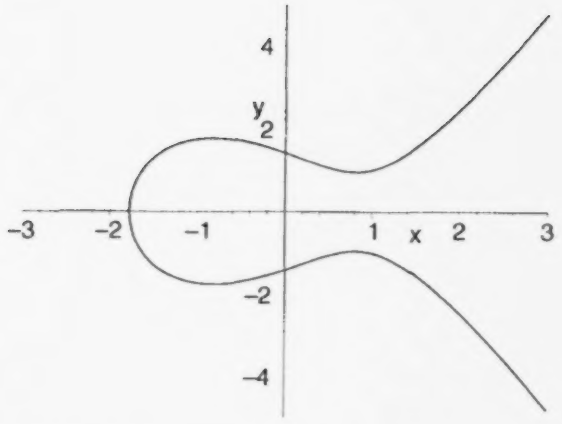

FIG 2 – Représentation cartésienne de la courbe elliptique $y^2 = x^3 - 2x + 2$

(ou bas) sur l'axe des y. C'est pourquoi on l'appelle souvent le point à l'infini □

Le théorème précédent nous apprend que chaque courbe elliptique peut s'écrire sous la forme de Weierstrass (2). Cependant, plusieurs équations de Weierstrass différentes peuvent représenter la même courbe elliptique (à un isomorphisme près) Par exemple, les courbes elliptiques $E_1 : y^2 + 6xy + 2y = x^3 - x + 5$ et $E_2 : y^2 = x^3 - x + 3$ sur le corps $\mathbb{F}_7$ sont isomorphes et toutes les deux sous la forme de Weierstrass. On peut voir qu'elles sont isomorphes en considérant le changement de variables $(x, y) \mapsto (x + 3, 3x + y + 1)$ qui envoie E_1 sur E_2.

PROPOSITION 3.1 Soit K un corps de caractéristique p et soit E une courbe elliptique sur K.

1) Si $p \neq 2, 3$, alors E est isomorphe à une courbe de la forme

$$y^2 = x^3 + ax + b.$$

2) Si $p = 2$, alors E est isomorphe à une courbe de la forme

$$y^2 + cy = x^3 + ax + b \qquad \text{ou} \qquad y^2 + xy = x^3 + ax^2 + b.$$

3) Si $p = 3$, alors E est isomorphe à une courbe de la forme

$$y^2 = x^3 + ax + b \qquad \text{ou} \qquad y^2 = x^3 + ax^2 + b.$$

Ces formes portent le nom de *formes normales de Weierstrass*

À partir d'une équation de Weierstrass, il existe un moyen simple pour savoir si la courbe est non singulière et donc si elle définit une courbe elliptique. L'outil utilisé est le discriminant de la courbe. Aussi, pour deux courbes données sous la forme de Weierstrass il est possible de reconnaître si celles-ci sont isomorphes. On introduit pour se faire la notion de j-invariant.

DÉFINITION 3 6 Soit E l'équation de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Le *discriminant* Δ de E est le nombre

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

et le *j-invariant* de E est le nombre

$$j := c_4^3/\Delta,$$

où

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, & c_4 &:= b_2^2 - 24b_4, \\ b_4 &:= 2a_4 + a_1a_3 & c_6 &:= -b_2^3 + 36b_2b_4 - 216b_6. \\ b_6 &:= a_3^2 + 4a_6, \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

On a le théorème suivant.

THÉORÈME 3 2

1) Une courbe définie par une équation de Weierstrass est non singulière si et seulement si $\Delta \neq 0$

2) Deux courbes elliptiques données par des équations de Weierstrass sont isomorphes si et seulement si elles ont le même j-invariant

EXEMPLE 3 5 La courbe $y^2 = (x-1)^2(x+5)$ sur $\mathbb{Q}$ est évidemment singulière puisqu'elle ne possède pas de tangente en $x = 1$ (elle a un zéro double en ce point) On vérifie qu'elle est singulière en calculant le déterminant de la courbe. Puisque

$$y^2 = (x-1)^2(x+5) = x^3 + 3x^2 - 9x + 5.$$

on a ici $a_1 = a_3 = 0$, $a_2 = 3$, $a_4 = -9$ et $a_6 = 5$ En remplaçant dans la formule du déterminant, on trouve

$$\begin{aligned} \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ &= -(12)^2(-21) - 8(-18)^3 - 27(20)^2 + 9(12)(-18)(20) \\ &= 0, \end{aligned}$$

P517601.PDF [Page: 33 of 64]

ce qui est en accord avec le théorème. □

EXEMPLE 3 6 Un calcul des j-invariants des courbes $E_1 : y^2+6xy+2y = x^3-x+5$ et $E_2 : y^2 = x^3-x+3$ sur $\mathbb{F}_7$ montre que $j(E_1) = 4$ et $j(E_2) = 4$. Ainsi, par le théorème, les courbes sont isomorphes, ce qui confirme la discussion précédente à ce sujet. □

3.3 Structure de groupe

Comme annoncé précédemment, nous allons maintenant voir que les courbes elliptiques possèdent une structure de groupe. C'est cet aspect en particulier qui les rend intéressantes pour les applications cryptographiques.

3.3.1 Courbe elliptiques sur $\mathbb{R}$

Dans un premier temps, considérons une courbe elliptique E sur $\mathbb{R}$ donnée sous la forme d'une équation de Weierstrass normale

$$E : y^2 = x^3 + ax + b \qquad (\Delta = -16(4a^3 + 27b^2) \neq 0).$$

Soient P et Q deux points sur E. Construisons la droite L passant par les points P et Q. Cette droite intersecte la courbe E en un troisième point R. Prenons maintenant la réflexion de R au travers l'axe des x. Ce nouveau point de E est noté $P + Q$. La figure 3 illustre la situation.

Muni de cette somme, l'ensemble des points de la courbe elliptique forme un groupe commutatif. Pour démontrer ce fait, il faut d'abord définir la somme $P+Q$ pour chaque paire (P, Q) d'éléments de E, et ensuite démontrer que les 4 axiomes d'un groupe commutatif sont satisfaits. Nous n'entrerons pas dans les détails de cette démonstration. Mais voici à tout le moins, une définition rigoureuse de l'addition.

DÉFINITION 3 7 Pour chaque $P \in E(\mathbb{R})$, on définit $\mathcal{O} + P = P + \mathcal{O} := P$. Ainsi, $\mathcal{O}$ sera l'élément neutre du groupe. En conséquence, on pose $-\mathcal{O} := \mathcal{O}$. Pour chaque $P \in E(\mathbb{R}) \setminus \{\mathcal{O}\}$, on définit $-P$ comme étant la la réflexion de P au travers l'axe des x. Évidemment, $-P$ est un point de E puisque cette dernière est symétrique par rapport à l'axe des x. Supposons maintenant que P et Q sont différents de $\mathcal{O}$. Pour définir $P + Q$, on distincte trois possibilités.

1) *P et Q ont des abscisses distinctes*

   On construit la droite L passant par P et Q. Si L est tangente au graphe en P, alors $P + Q = P$. Si L est tangente au graphe en Q, alors $P + Q = Q$. Dans les

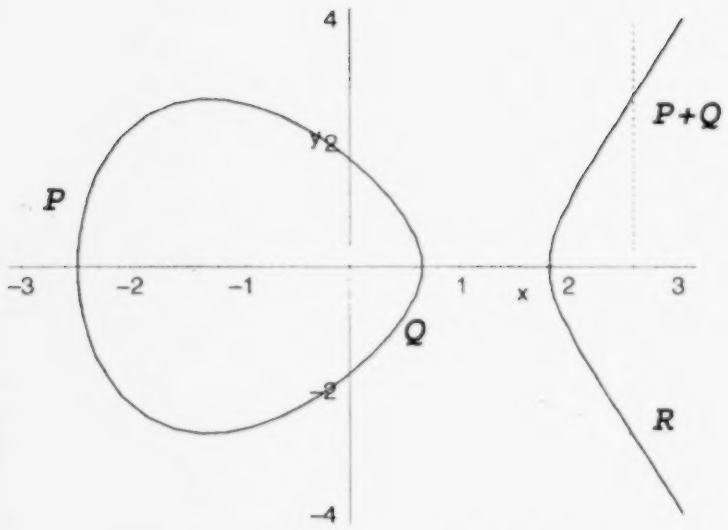

FIG 3 - Addition sur une courbe elliptique.

autres cas. L intersecte la courbe E en exactement un autre point R. On définit $P + Q := -R$.

2) $P = -Q$

On pose $P + Q = \mathcal{O}$

3) $P = Q$ et $P \neq -Q$

On construit la droite L tangente au graphe en P. Celle-ci intersecte la courbe en exactement un autre point R. On pose $P + Q := -R$

Cette définition de la somme de deux points est très géométrique. Elle permet donc de bien visualiser la transformation $(P, Q) \mapsto P + Q$. Elle permet aussi de démontrer facilement les axiomes d'un groupe commutatif sauf celui d'associativité qui demande plus de travail (voir par exemple [8, Theorem 2.46])

De cette définition, on peut extraire des formules algébriques permettant de calculer les coordonnées du point $P + Q$ en fonction de celles de P et Q. Posons $P := (x_0, y_0)$, $Q := (x_1, y_1)$ et $P + Q := (x_2, y_2)$. Supposons que nous sommes dans le cas 1 de la définition précédente (i.e. $x_0 \neq x_1$). Alors, l'équation de L est $y = \alpha x + \beta$ où $\alpha := \frac{y_1 - y_0}{x_1 - x_0}$ et $\beta := y_0 - \alpha x_0$. Un point de L de la forme $(x, \alpha x + \beta)$ est sur la courbe elliptique E si et seulement si il satisfait l'équation de celle-ci, c'est-à-dire si et seulement si $(\alpha x + \beta)^2 = x^3 + ax + b$. Cette cubique possède les solutions $x = x_0$ et $x = x_1$ puisque P et Q sont

des points de $L \cap E$. Or, il est fort connu que la somme des trois racines d'une équation cubique de la forme $x^3 + Ax^2 + Bx + C = 0$ est $-A$. Appliquée à notre situation, cette proposition donne $\alpha^2 = x_0 + x_1 + x_2$. Ainsi, on a

$$x_2 = \left(\frac{y_1 - y_0}{x_1 - x_0}\right)^2 - x_0 - x_1.$$

D'autre part, $y_2 = -(\alpha x_2 + \beta) = -\alpha x_2 - y_0 + \alpha x_0$ et donc,

$$y_2 = \left(\frac{y_1 - y_0}{x_1 - x_0}\right)(x_0 - x_2) - y_0$$

Si maintenant nous sommes dans le cas 3 de la définition (le cas 2) est une simple vérification), alors l'équation de L est $y = \alpha x + \beta$ où $\alpha = \left.\frac{\mathrm{d}y}{\mathrm{d}x}\right|_{x=x_0}$ et $\beta := y_0 - \alpha x_0$. Une dérivation implicite de l'équation de E montre que

$$y'(x_0) = \frac{3x_0^2 + a}{2y_0}.$$

Par conséquent, on trouve

$$\begin{aligned} x_2 &= \left(\frac{3x_0^2 + a}{2y_0}\right)^2 - 2x_0, \\ y_2 &= \left(\frac{3x_0^2 + a}{2y_0}\right)(x_0 - x_2) - y_0. \end{aligned}$$

En résumé, nous avons montré ce qui suit. Soit E une courbe elliptique sur $\mathbb{R}$ d'équation $y^2 = x^3 + ax + b$ et soient $P := (x_0, y_0)$ et $Q := (x_1, y_1)$ deux points de E. Alors les coordonnées de $P + Q := (x_2, y_2)$ peuvent être calculées selon le tableau 1

3.3.2 Courbes elliptiques sur $\mathbf{F}_{p^n}$ $(p > 3)$

L'approche géométrique utilisée dans le cas où les courbes elliptiques sont définies sur le corps $\mathbb{R}$ n'est plus applicable dans le cas d'un corps fini. Malgré tout, il est toujours possible de définir une structure de groupe sur une courbe elliptique, et ce peu importe le corps sous-jacent. L'idée est que les formules du tableau de la section précédente sont des expressions algébriques calculables non seulement dans $\mathbb{R}$, mais aussi dans n'importe quel corps de caractéristique différente de 2 (à cause des dénominateurs dans la dernière ligne du tableau). Ces formules peuvent donc servir de définition.

Sachant que l'équation d'une courbe elliptique sur un corps fini de caractéristique supérieure à 3 peut toujours s'écrire sous la forme $y^2 = x^3 + ax + b$, on définit ainsi l'addition de deux points P et Q sur une courbe elliptique E sur $\mathbf{F}_{p^n}$ $(p > 3)$ par le tableau ci-haut.

$P = \mathcal{O}$	$P + Q = Q$
$Q = \mathcal{O}$	$P + Q = P$
$x_0 \neq x_1$	$x_2 = \left(\frac{y_1 - y_0}{x_1 - x_0}\right)^2 - x_0 - x_1$ $y_2 = \left(\frac{y_1 - y_0}{x_1 - x_0}\right)(x_0 - x_2) - y_0$
$x_0 = x_1$ et $y_0 = -y_1$	$P + Q = \mathcal{O}$
$x_0 = x_1$ et $y_0 = y_1 \neq 0$	$x_2 = \left(\frac{3x_0^2 + a}{2y_0}\right)^2 - 2x_0,$ $y_2 = \left(\frac{3x_0^2 + a}{2y_0}\right)(x_0 - x_2) - y_0.$

TAB 1 - Addition de points sur la courbe elliptique $y^2 = x^3 + ax + b$ sur $\mathbb{R}$

Voyons immédiatement un exemple de ceci.

EXEMPLE 3 7 Considérons la courbe $E : y^2 = x^3 + (10)x + (02)$ sur le corps $\mathbb{F}_{5^2}$ dont la représentation est en base polynomiale modulo $t^2 + 2$ Le discriminant de cette courbe est $\Delta = -16(4a^3 + 27b^2) = (32) \neq 0$. Il s'agit donc bien d'une courbe elliptique. Un calcul direct montre que le point $\alpha := ((00)\ (20))$ est sur la courbe E En effet

$$y^2 = (20)^2 = 4t^2 \equiv 4(-2) \equiv 2 = (02) = x^3 + (10)x + (02).$$

En utilisant les formules d'additions, on trouve les multiples successifs de α

$$\alpha = ((00), (20)). \qquad 2\alpha = ((01), (31)). \qquad 3\alpha = ((23), (31)),$$
$$\cdots$$
$$26\alpha = ((01), (24)) \qquad 27\alpha = ((00), (30)), \qquad 28\alpha = \mathcal{O}.$$

Puisque 28 est le premier multiple non nul de α qui donne l'élément neutre du groupe, on en déduit que α est un élément d'ordre 28 On sait alors que l'ordre du groupe $|E(\mathbb{F}_{5^2})|$ est un multiple de 28. Or, il est clair que $|E(\mathbb{F}_{5^2})| \leq 50$ puisque pour chaque x possible (25 cas) il y a au plus 2 valeurs de y qui satisfont l'équation de la courbe En conséquence, $|E(\mathbb{F}_{5^2})| = 28$ et l'élément α est un générateur du groupe On a donc montré que $E(\mathbb{F}_{5^2})$ est le groupe cyclique d'ordre 28 (i e isomorphe à $\mathbb{Z}_{28}$) □

EXEMPLE 3 8 Regardons maintenant la courbe elliptique $E : y^2 = x^3 - 3x - 1$ sur le corps $\mathbb{F}_{17}$ Les seuls éléments de $\mathbb{F}_{17}$ qui admettent des racines carrées dans ce corps

sont 0, ± 1, ± 2, ± 4 et ± 8. En substituant chaque valeur possible pour x dans l'équation de E, on identifie facilement les 20 points de cette courbe, à savoir

$$\begin{aligned} E(\mathbb{F}_{17}) = \{&\mathcal{O}, (0,4), (0,13), (2,1), (2,16), (3,0), (4,0), (7,7), (7,10), (9,2), \\ &(9,15), (10,0), (12,5), (12,12), (13,7), (13,10), (14,7), (14,10), \\ &(16,1), (16,16)\}. \end{aligned}$$

Si on calcule l'ordre de chacun de ces éléments, on trouve le tableau suivant.

$\lvert\mathcal{O}\rvert = 1$	$\lvert(0,4)\rvert = 10$	$\lvert(0,13)\rvert = 10$	$\lvert(2,1)\rvert = 5$
$\lvert(2,16)\rvert = 5$	$\lvert(3,0)\rvert = 2$	$\lvert(4,0) = 2$	$\lvert(7,7)\rvert = 10$
$\lvert(7,10)\rvert = 10$	$\lvert(9,2)\rvert = 10$	$\lvert(9,15) = 10$	$(10,0)\rvert = 2$
$\lvert(12,5)\rvert = 5$	$\lvert(12,12)\rvert = 5$	$\lvert(13,7) = 10$	$\lvert(13,10)\rvert = 10$
$\lvert(14,7)\rvert = 10$	$\lvert(14,10)\rvert = 10$	$\lvert(16,1) = 10$	$\lvert(16,16) = 10$

Évidemment, l'ordre de chaque élément divise l'ordre du groupe. Ce que l'on remarque toutefois, c'est qu'aucun élément n'est d'ordre 20, c'est-à-dire que ce groupe ne possède pas de générateur. Il s'agit donc d'un groupe non cyclique. En fait, on peut montrer que ce groupe est isomorphe au groupe $\mathbf{Z}_{10} \times \mathbf{Z}_2$. □

3.3.3 Courbes elliptiques sur $\mathbb{F}_{2^n}$ et $\mathbb{F}_{3^n}$.

On a vu que dans le cas d'une courbe elliptique sur un corps de caractéristique 2 ou 3, les équations de Weierstrass sont légèrement différentes du cas général. En conséquence, les formules d'addition sont elles aussi différentes. On peut les déduire en considérant l'approche géométrique des courbes sur $\mathbb{R}$.

Afin de limiter les listes de formules, nous allons discuter ici que des équations de la forme $y^2 + xy = x^3 + ax^2 + b$ sur $\mathbb{F}_{2^n}$. Il s'agit du seul cas d'intérêt (parmi les corps de caractéristique 2 ou 3) en cryptographie.

Soit E une courbe elliptique sur $\mathbb{F}_{2^n}$ d'équation $y^2 + xy = x^3 + ax^2 + b$ et soient $P := (x_0\ y_0)$ et $Q := (x_1, y_1)$ deux points de E. Alors les coordonnées de $P + Q := (x_2, y_2)$ peuvent être calculées selon le tableau 2.

EXEMPLE 3.9 Considérons la courbe elliptique $E : y^2 + xy = x^3 + 1$ sur $\mathbb{F}_{2^5}$. Il s'agit bien d'une courbe elliptique puisque son discriminant est non nul ($\Delta = 1$). Dans la représentation modulo $t^4 + t^2 + 1$, posons $\alpha := ((00100), (10010))$. On vérifie aisément qu'il s'agit d'un point de la courbe E. Calculons quelques multiples de α. Pour calculer $2\alpha = \alpha + \alpha$, il faut utiliser la dernière ligne du tableau. Ainsi,

$$\begin{aligned} x_2 &= (00100)^2 + \frac{1}{(00100)^2} = (10000) + \frac{1}{(10000)} \\ &= (10000) + (01011) = (11011) \end{aligned}$$

$P = \mathscr{O}$	$P + Q = Q$
$Q = \mathscr{O}$	$P + Q = P$
$x_0 \neq x_1$	$x_2 = \left(\frac{y_0 + y_1}{x_0 + x_1}\right)^2 + \frac{y_0 + y_1}{x_0 + x_1} + x_0 + x_1 + a$ $y_2 = \left(\frac{y_0 + y_1}{x_0 + x_1}\right)(x_0 + x_2) + x_2 + y_0$
$x_0 = x_1$ et $y_0 = x_1 + y_1$	$P + Q = \mathscr{O}$
$x_0 = x_1 \neq 0$ et $y_0 = y_1$	$x_2 = x_0^2 + \frac{b}{x_0^2}$, $y_2 = x_0^2 + \left(1 + x_0 + \frac{y_0}{x_0}\right) x_2$.

TAB 2 – Addition de points sur la courbe elliptique $y^2 + xy = x^3 + ax^2 + b$ sur $\mathbb{F}_{2^N}$.

et

$$\begin{aligned} y_2 &= (00100)^2 + \left(1 + (00100) + \frac{(10010)}{(00100)}\right)(11011) \\ &= (10000) + ((00101) + (10010)(01001))\,(11011) \\ &= (10000) + (10011)(11011) \\ &= (10100) \end{aligned}$$

On peut vérifier que ce point est bel et bien sur la courbe E. En utilisant cette fois-ci la troisième ligne du tableau, on montre que

$$3\alpha = 2\alpha + \alpha = ((11011), (10100)) + ((00100), (10010)) = ((00010)\ (11111)).$$

Deux applications successives du doublement de point donnent

$$12\alpha = 2(2(3\alpha))) = 2((01101), (00110)) = ((00100), (10010)).$$

Ainsi, $12\alpha = \alpha$ et donc, $11\alpha = 0$. Par conséquent, α est un élément d'ordre 11 dans le groupe $E(\mathbb{F}_{2^5})$. Ainsi, l'ordre de E est un multiple de 11. En fait, on peut montrer que $|E| = 44$ et qu'il s'agit d'un groupe cyclique. □

4 Problème du logarithme discret

Le problème du logarithme discret (PLD) est à la base de la sécurité de plusieurs protocoles cryptographiques. Parmi ceux-ci, notons le protocole d'échange de clés Diffie-Hellman, le protocole de cryptage ElGamal et le protocole de signature électronique ElGamal. La sécurité de ces protocoles se traduit mathématiquement par le fait que le problème du logarithme discret est difficile à résoudre.

4.1 Définition

DÉFINITION 4.1 Soient G un groupe cyclique d'ordre n, α un générateur de G et β un élément de G. Trouver un entier $x \in \{0, 1, \ldots, n-1\}$ tel que $\alpha^x = \beta$. Cet entier x s'appelle le *logarithme discret* de β dans la base α et est noté $x = \log_\alpha \beta$.

Le problème du logarithme discret, tel qu'énoncé ci-haut, admet toujours une et une seule solution.

EXEMPLE 4.1 Soit G le groupe $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$. Il s'agit d'un groupe cyclique puisque $\alpha := 5$ est un générateur du groupe. Le logarithme discret de $\beta := 13$ dans la base α est 4 puisque $5^4 \equiv 13 \bmod 18$. On peut donc écrire $\log_5 13 = 4$. □

4.2 Groupes d'intérêt en cryptographie

Les applications cryptographiques classiques qui utilisent les logarithmes discrets se font la plupart du temps dans le groupe multiplicatif d'un corps fini $\mathbb{F}_q$ (voir par exemple [9, 10]). En pratique les groupes $\mathbb{Z}_p^*$ et $\mathbb{F}_{2^n}^*$ sont les plus convoités en raison de leur efficacité lors de mises en application concrètes.

Parmi les autres types de groupes qui ont été proposés pour des applications cryptographiques, on retrouve

- les groupes d'unités $\mathbb{Z}_n^*$ où n est un entier composé (voir [11]);
- les groupes induits par des courbes elliptiques sur des corps finis (voir [12, 13]) et
- les groupes induits par le jacobien des courbes hyperelliptiques sur des corps finis (voir [14]).

Pour être intéressant un groupe doit satisfaire au minimum les deux conditions suivantes

- **efficacité:** les opérations de groupe doivent être relativement simples;
- **sécurité:** le PLD doit être difficile dans ce groupe.

Les algorithmes connus pour résoudre le PLD ne sont pas tous du même type. Il y a des algorithmes qui fonctionnent dans tous les groupes et d'autres qui sont spécialisés à certains types de groupes. Selon le groupe dans lequel on travaille, la difficulté du problème du logarithme discret n'est donc pas toujours la même. D'où l'intérêt de la deuxième condition ci-haut.

4.3 Comparaison entre différents PLD

Les groupes induits par des courbes elliptiques sont intéressants parce qu'ils satisfont les critères d'efficacité et de sécurité. En comparaison avec les techniques classiques qui utilisent les groupes $\mathbb{F}_q^*$, les courbes elliptiques sont moins efficaces (les opérations sont plus complexes), mais offrent une bien meilleure sécurité. La raison de cette sécurité accrue est que le meilleur algorithme connu pour la résolution du PLD sur les courbes elliptiques est un algorithme non spécialisé pouvant s'appliquer à n'importe quel groupe cyclique général. Il s'agit d'une variante de l'algorithme rhô de Pollard (*Pollard's rho algorithm* - pour plus de détails voir [15, 16, 17, 18, 19]). Or, dans les groupes de type $\mathbb{F}_q^*$, on connaît des algorithmes spécialisés plus performants, comme par exemple l'algorithme de calcul indiciel (*index-calculus algorithm*). Pour des détails sur celui-ci, voir entre autres [20, 21, 22].

Soit G un groupe cyclique et soit $n := |G|$. L'espérance du temps d'exécution de l'algorithme *Pollard's rho* est $O(\sqrt{n})$. Cela signifie que le temps d'exécution de l'algorithme croît asymptotiquement comme $\sqrt{n}$ lorsque n tend vers l'infini. Notons par $k := \log_2 n$ le nombre (approximatif) de bits de n. Alors on peut écrire que l'espérance du temps d'exécution est $O\left(\sqrt{2^k}\right)$, ou encore $O\left(2^{k/2}\right)$. On dit de l'algorithme *Pollard's rho* qu'il a un temps d'exécution exponentiel. Chaque 2 bits supplémentaires de n double le temps d'exécution de l'algorithme.

Soit maintenant le groupe cyclique $G := \mathbb{F}_q^*$, où q est soit une puissance de 2, soit un nombre premier. L'espérance du temps d'exécution de l'algorithme *index-calculus* est $L_q[\frac{1}{3}, c]$ pour une certaine constante $c > 0$ où

$$L_q[\alpha, c] := O\left(e^{(c+o(1))(\ln q)^\alpha (\ln \ln q)^{1-\alpha}}\right).$$

En écrivant $k := \ln q$, on a

$$L_q[\frac{1}{3}, c] = O\left(e^{(c+o(1))k^{1/3}(\ln k)^{2/3}}\right).$$

P517601.PDF [Page: 41 of 64]

Ainsi, l'algorithme du calcul indiciel a un temps d'exécution qui est sous-exponentiel Pour les autres groupes du type $\mathbb{F}_q^*$, il est conjecturé que l'algorithme s'exécute également en temps sous-exponentiel (voir [23, 24])

Donc, en pratique, il est plus facile de résoudre un PLD dans $\mathbb{F}_q^*$ que dans un groupe où le meilleur algorithme connu est *Pollard's rho*. Les groupes induits par des courbes elliptiques sont dans cette dernière classe, d'où leur intérêt en cryptographie

5 Protocoles cryptographiques

Nous allons maintenant regarder de quelle manière le problème du logarithme discret sur les courbes elliptiques est exploité en cryptographie. Les protocoles cryptographiques utilisant les courbes elliptiques sont nombreux et en constante évolution (voir section 7). Le but de cette section n'est pas de faire la liste complète de ces protocoles qui se retrouvent dans différentes normes internationales, mais plutôt d'en exhiber quelques uns, dans leurs grandes lignes, afin de comprendre le lien entre la pratique et la théorie.

Les protocoles que nous allons décrire dans cette section sont tirés de la norme SEC 1 du SECG (*Standards for Efficient Cryptography Group*, voir page 39 et [25]). Nous avons choisi un protocole de signature électronique, un de cryptage et un d'échange de clés. Notons que dans chaque cas, il s'agit d'une version simplifiée d'un protocole apparaissant dans [25].

5.1 Elliptic Curve Digital Signature Algorithm (ECDSA)

La situation est la suivante. Un individu A veut transmettre un message m à un autre individu B, de sorte que les propriétés suivantes soient satisfaites.

- *Authentification d'origine.* B est assuré de la provenance de m, c'est-à-dire que personne autre que A n'a pu signer ce message.
- *Intégrité.* B est assuré que le message m n'a pu être modifié depuis la signature de A.
- *Non répudiation.* B peut prouver à une tierce partie que A a signé le message m.

L'algorithme de signature électronique ECDSA présenté ci-après fournit ces trois services cryptographiques. Nous allons le décrire en quatre étapes : les paramètres du schéma, la construction des clés, la signature d'un message et la vérification d'une signature.

On note par $\{0,1\}^*$ l'ensemble des suites binaires finies et on suppose que le message m à signer est un élément de $\{0,1\}^*$.

- **Paramètres du schéma.**
  1) Sélectionner une courbe elliptique $E(\mathbb{F}_q)$ et un point P sur cette courbe dont l'ordre n est un nombre premier.
  2) Fixer une fonction injective $f : \mathbb{F}_q \to \mathbb{Z}$. Il s'agit d'une représentation binaire des éléments du corps $\mathbb{F}_q$.

3) Choisir une fonction de hachage $h : \{0,1\}^* \to \mathbb{Z}_n$

- **Construction de la clé publique et de la clé privée de A.**

1) Choisir un entier aléatoire a tel que $2 \leq a \leq n-1$
2) Calculer $Q := aP$

Clé publique de A: (P, Q),	Clé privée de A a.

- **Signature du message m par A.**

1) Choisir un entier aléatoire k tel que $2 \leq k \leq n-1$.
2) Calculer $R := (x_R, y_R) := kP$.
3) Calculer $r := f(x_R) \bmod n$ Si $r = 0$ alors retourner à l'étape 1.
4) Calculer $s := k^{-1}[h(m) + ar] \bmod n$ Si $s = 0$ alors retourner à l'étape 1.

Signature de A pour le message m. (r, s).

- **Vérification de la signature par B.**

1) Calculer $u_1 := h(m)s^{-1} \bmod n$
2) Calculer $u_2 := rs^{-1} \bmod n$.
3) Calculer $T := (x_T, y_T) := u_1 P + u_2 Q$.
4) Calculer $v := f(x_T) \bmod n$

La signature est acceptée si et seulement si $v = r$

On vérifie facilement que si A et B suivent l'algorithme ci-haut, alors $v = r$ En effet, on a

$$T = u_1 P + u_2 Q = h(m)s^{-1}P + rs^{-1}aP = s^{-1}[h(m) + ra]P = kP = R.$$

Ainsi, $x_T = x_R$ et donc $v = r$. D'autre part, un adversaire voulant forger la signature de A sur un message m doit trouver r et s tels que $v = r$, c'est-à-dire tels que

$$f\left(\left[s^{-1}(h(m)P + rQ)\right]_x\right) = r, \qquad (\star)$$

où $[\cdot]_x$ est la composante en x. Évidemment, s'il connaît la clé secrète a, alors il peut utiliser le même algorithme que A pour résoudre $(\star)$ Il est donc essentiel que la clé privée de A soit connue de lui seul Si l'adversaire ne connaît pas la clé privée de A, il peut soit tenter de la retrouver à partir de la clé publique $(P, Q) = (P, aP)$, ou soit tenter de résoudre directement $(\star)$ pour r et s Dans le premier cas il s'agit du problème du logarithme discret. Dans le second cas, il semble que peu d'options soient envisageables. La seule technique connue à ce jour est celle de fixer r et de résoudre $(\star)$ pour s Il s'agit encore une fois d'un PLD.

Ainsi, il est essentiel pour la sécurité de ce protocole que le PLD dans le groupe $E(\mathbb{F}_q)$ soit difficile à résoudre C'est la difficulté de ce problème qui empêche un adversaire de forger une signature à la place de A

Il n'a pas été démontré formellement que la résolution de $(\star)$ est équivalente au problème du logarithme discret. Il existe peut-être une manière plus facile de trouver r et s qui n'implique pas la résolution d'un PLD. Il s'agit d'une question toujours ouverte

La relation entre le problème du logarithmediscret et la sécurité du protocole ECDSA de signature électronique peut ne pas sembler satisfaisante parce qu'on ne sait pas s'il existe un moyen de contourner la difficulté du PLD Toutefois, il est à noter qu'une telle ignorance est omniprésente en cryptographie Par exemple, le célèbre protocole RSA base sa sécurité sur le fait qu'il est difficile de factoriser les grands nombres. Or, il n'a jamais été démontré qu'il faut absolument savoir factoriser pour briser RSA

Ces constatations montrent que la sécurité des protocoles cryptographiques est directement tributaire des connaissances mathématiques et algorithmiques actuelles Une percée dans une direction ou une autre pourrait faire s'effondrer une grande partie de ce qui est considéré aujourd'hui comme sécuritaire

5.2 Elliptic Curve Integrated Encryption Scheme (ECIES)

La version de l'algorithme de cryptage ECIES présentée ci-après offre le service cryptographique de *confidentialité*. Elle permet à un individu B d'envoyé un message crypté à un individu A de sorte que seul A puisse décrypter ce message

L'algorithme n'impose aucune restriction sur la longueur du message à crypter Le message peut simplement n'être qu'une clé qui sera utilisée ultérieurement lors d'une session cryptée par un algorithme à clés symétriques Mais il peut aussi être constitué d'une quantité importante de données Le protocole utilise, pour crypter le message, un algo-

rithme à clés symétriques, ce qui lui permet d'être performant même dans le cas de longs messages

Dans le protocole qui suit, seul A doit posséder une paire de clés. Pour construire celle-ci, il procède comme dans le cas de l'algorithme de signature électronique précédent.

On suppose que le message à crypter m est un élément de $\{0,1\}^*$.

- **Paramètres du schéma.**

  1) Sélectionner une courbe elliptique $E(\mathbb{F}_q)$ et un point P sur cette courbe dont l'ordre n est un nombre premier

  2) Choisir un algorithme de cryptage à clés symétriques $Cry : K \times \{0,1\}^* \to \{0,1\}^*$, où K est l'ensemble des clés admissibles. L'algorithme de décryptage associé est noté Dec.

  3) Fixer une fonction de hachage $h : E(\mathbb{F}_q) \to K$

- **Construction de la clé publique et de la clé privée de A.**

  1) Choisir un entier aléatoire a tel que $2 \leq a \leq n-1$

  2) Calculer $Q := aP$

Clé publique de A (P, Q),	Clé privée de A: a.

- **Cryptage du message m par B.**

  1) Choisir un entier aléatoire k tel que $2 \leq k \leq n-1$.

  2) Calculer $R := kP$.

  3) Calculer $z := h(kQ)$

  4) Calculer $e := Cry(z, m)$

Message crypté: (R, e).

- **Décryptage du message (R, e) par A.**

  1) Calculer $Dec(h(aR), e)$.

$$\boxed{m = Dec(h(aR), e).}$$

Pour vérifier que le protocole fonctionne, voyons d'abord que l'affirmation du dernier encadré est vraie. Puisque $R = kP$, $Q = aP$ et que $Dec(z, \cdot)$ est la fonction inverse de $Cry(z, \cdot)$, on a

$$Dec(h(aR), e) = Dec(h(akP), e) = Dec(h(kQ), e) = Dec(z, Cry(z, m)) = m$$

Ainsi, le détendeur de la clé privée a peut retrouver le message m à partir de (R, e). D'autre part, un adversaire ne connaissant pas a est confronté au problème $(\star)$ de calculer akP ne connaissant que $R = kP$ et $Q = aP$. Celui-ci devient trivial si cet adversaire peut calculer le logarithme discret de Q en base P. Il est donc essentiel pour la sécurité de cet algorithme que le PLD soit difficile à résoudre dans le groupe $E(\mathbb{F}_q)$

Le problème $(\star)$ est connu sous le nom de *problème de Diffie-Hellman*. Il peut être énoncé dans un groupe cyclique quelconque. Le problème de Diffie-Hellman n'est évidemment pas plus difficile que celui du logarithme discret puisque si on sait résoudre ce dernier alors le premier devient trivial. La question qui demeure ouverte est celle de savoir si les deux problèmes sont équivalents du point de vue de la complexité algorithmique. Cette équivalence a été démontrée dans certains cas où on possède de l'information sur la factorisation de l'ordre du groupe (ces résultats sont cités dans [26, page 114]). Elle a aussi été démontrée dans le cas des groupes sur des courbes elliptiques (voir [27, section 4.3]). Ainsi, s'il existe un algorithme sous-exponentiel permettant de résoudre le problème de Diffie-Hellman sur une courbe, il existe aussi un algorithme sous-exponentiel permettant de résoudre le PLD dans ce groupe

5.3 Elliptic Curve Diffie-Hellman Scheme (ECDHS)

Une des difficultés rencontrées dans les applications utilisant des algorithmes de cryptage à clés symétriques est de trouver une méthode pour construire et partager la clé privée commune qui sera utilisée. Plusieurs techniques pour résoudre ce problème sont basées sur le protocole d'échange de clés de Diffie-Hellman dont la sécurité repose sur le problème du logarithme discret. Les idées de ce protocole apparaissent dans le papier original de Diffie et Hellman [28]

Nous allons présenter ici une version adaptée aux courbes elliptiques. Le contexte est celui de deux individus A et B qui veulent établir une communication (dans un milieu hostile) dans laquelle les messages seront cryptés à l'aide d'une clé privée K. L'étape considérée ici est celle de construire et partager cette clé K de sorte qu'elle ne soit connue que de A et B seulement

Pour établir cette clé, les deux parties utilisent des clés privées et publiques. Un adversaire n'ayant accès qu'à l'information échangée et aux clés publiques des parties A et B, est confronté, pour construire K, au difficile problème de Diffie-Hellman

- **Paramètres du schéma.**
  1) Sélectionner une courbe elliptique $E(\mathbb{F}_q)$ et un point P sur cette courbe dont l'ordre n est un nombre premier
  2) Fixer une fonction de hachage h définie sur $E(\mathbb{F}_q)$ et dont les valeurs sont les clés symétriques admissibles

- **Construction des clés publiques et privées de A et B.**
  1) A choisit un entier aléatoire a tel que $2 \leq a \leq n-1$.
  2) A transmet $Q_A := aP$ à B
  3) B choisit un entier aléatoire b tel que $2 \leq b \leq n-1$.
  4) B transmet $Q_B := bP$ à A.

- **Construction de la clé symétrique commune.**
  1) A calcule $K := h(aQ_B)$.
  2) B calcule $K := h(bQ_A)$

À la fin du protocole, A et B possèdent tous deux la même clé secrète $K = h(abP)$ Un adversaire qui ne voit que les messages que A et B s'échangent fait face au problème de trouver abP ne sachant que aP et bP Comme on l'a vu dans la section précédente, ce problème est celui de Diffie-Hellman Ce problème n'est pas plus difficile que le PLD en général et les deux sont équivalents dans le cas des courbes elliptiques (voir section 5 2)

6 Courbes elliptiques particulières

La sécurité de la cryptographie sur courbes elliptiques (ECC - *Elliptic Curve Cryptography*) est basée sur la difficulté à résoudre le problème du logarithmediscret dans les groupes $E(\mathbb{F}_{p^n})$ Le meilleur algorithme connu pour résoudre ce problème est une variation de la méthode rhô de Pollard obtenue par [17] Le temps d'exécution de cet algorithme est exponentiel

Sur certaines courbes elliptiques particulières, il existe des méthodes spécifiques pouvant améliorer la vitesse de résolution du PLD. Lorsque le temps d'exécution peut être suffisamment amélioré, il est recommandé de ne pas utiliser ces courbes dans des protocoles cryptographiques En particulier, les courbes pour lesquelles il existe des algorithmes sous-exponentiels sont à proscrire Voici l'ensemble des courbes elliptiques particulières pour lesquelles des techniques plus performantes que celle de Pollard sont connues

6.1 Courbes elliptiques super-singulières

Il a été démontré (voir [29]) que le problème du logarithmediscret dans le groupe $E(\mathbb{F}_q)$ peut être réduit au problème du logarithmediscret dans le groupe $\mathbb{F}_{q^k}^*$ pour un certain entier positif k Sachant que ce dernier est plus facile à résoudre que le premier (à cause de la méthode du calcul indiciel qui s'applique), il est essentiel de s'assurer que l'entier k est suffisamment grand (pour la courbe E en question) de sorte que le problème du logarithmediscret dans $\mathbb{F}_{q^k}^*$ demeure très difficile. La plupart des courbes elliptiques possèdent un k suffisamment élevé (voir [30, 31]).

Une méthode pratique pour vérifier que l'algorithme de réduction ne s'applique pas à une courbe elliptique particulière E consiste à vérifier que $|E|$ ne divise pas $q^k - 1$ pour chaque k pour lequel le problème du logarithmediscret dans $\mathbb{F}_{q^k}^*$ est résoluble en pratique. En effet, pour que $E(\mathbb{F}_q)$ puisse être immergé dans le groupe $\mathbb{F}_{q^k}^*$, il faut que $|E(\mathbb{F}_q)|$ divise $q^k - 1$. De plus, sous de faibles hypothèses, cette condition est également suffisante ([31]).

La *trace* d'une courbe elliptique E est l'entier $t := p^n + 1 - |E(\mathbb{F}_{p^n})|$ Une courbe elliptique est dite *super-singulière* si sa trace t est divisible par la caractéristique p du corps sous-jacent. Pour cette classe particulière de courbes, il est connu que $k \leq 6$ Ainsi, la méthode de réduction fournit dans ce cas un algorithme sous-exponentiel pour extraire des logs discrets dans $E(\mathbb{F}_{p^n})$. Ces courbes ne doivent donc pas être utilisées dans des protocoles cryptographiques

6.2 Courbes elliptiques anormales sur $\mathbb{Z}_p$

Une courbe elliptique E sur $\mathbb{Z}_p$ est dite *anormale* si $|E(\mathbb{Z}_p)| = p$. Les courbes $\mathbb{Z}_p$-anormales ont leurs traces égalent à 1. Il a été démontré (voir par exemple [32]) qu'un isomorphisme entre $E(\mathbb{Z}_p)$ et le groupe additif de $\mathbb{Z}_p$ peut être calculé de manière efficace Or, le PLD dans le groupe additif de $\mathbb{Z}_p$ est trivial. Ainsi, le PLD sur une courbe $\mathbb{Z}_p$-anormale peut être résolu en temps polynomial. Ces courbes sont donc à éviter Cette attaque ne semble pas s'adapter à d'autres courbes elliptiques. Il suffit donc de vérifier que la cardinalité d'une courbe E sur $\mathbb{Z}_p$ n'est pas p

6.3 Courbes elliptiques sur un sous-corps

Supposons que la courbe elliptique E est définie sur le corps $\mathbb{F}_{2^r}$ On peut alors voir la courbe E comme une courbe sur $\mathbb{F}_{2^{rd}}$ puisque $\mathbb{F}_{2^r}$ est un sous-corps de $\mathbb{F}_{2^{rd}}$ Il a été démontré (voir par exemple [17]) que l'algorithme *Pollard's rho* sur $E(\mathbb{F}_{2^{rd}})$ peut être accéléré d'un facteur $\sqrt{d}$

Le temps d'exécution (mesuré en nombres d'additions sur une courbe elliptique) de l'algorithme *Pollard's rho* est

$$\frac{\sqrt{\pi n}}{2} + O(\log n).$$

Avec l'accélération précédente, le temps d'exécution devient approximativement $\frac{\sqrt{\pi n/d}}{2}$

Les *courbes de Koblitz* sont des courbes elliptiques sur $\mathbb{F}_{2^n}$ dont les coefficients sont dans $\mathbb{Z}_2$. Il existe donc seulement deux courbes de Koblitz, à savoir

$$y^2 + xy = x^3 + 1 \quad \text{et} \quad y^2 + xy = x^3 + x^2 + 1.$$

Sur les courbes de Koblitz l'algorithme *Pollard's rho* s'exécute donc en $\frac{\sqrt{\pi 2^n/n}}{2}$ opérations.

6.4 Courbes elliptiques sur $\mathbb{F}_{2^m}$ où m est composé

Gaudry, Hess et Smart ont montré dans [33] qu'il existe des méthodes plus performantes que l'algorithme *Pollard's rho* dans le cas où m possède de petits diviseurs. Pour cette raison, il n'est pas recommandé d'utiliser des courbes elliptiques sur les corps $\mathbb{F}_{2^m}$ où m est composé.

6.5 Algorithme de Pohlig-Hellman

La technique de Pohlig et Hellman (voir [34]) exploite la factorisation de l'ordre n du groupe G dans lequel on veut calculer un logarithme discret. En effet, il suffit pour résoudre un PLD dans G de calculer le logarithme discret modulo chaque facteurs premiers de n. On peut ensuite reconstruire la solution du PLD à l'aide du théorème du reste chinois.

En conséquence, dans toutes les techniques cryptographiques basées sur le PLD, il est de mise d'éviter les groupes dont l'ordre ne possède que de petits facteurs premiers. Cela s'applique donc en particulier aux groupes de courbes elliptiques. Un moyen efficace d'éviter l'attaque Pohlig-Hellman est de choisir un groupe dont l'ordre (ou à tout le moins l'ordre du point de base considéré pour le PLD) est premier.

7 Normes régissant les SCCE

Parmi les éléments qui influencent le plus le déploiement à grande échelle d'un système cryptographique, on retrouve l'interopérabilité, la confiance du public et l'existence d'études techniques approfondies. L'interopérabilité est la portabilité et la mobilité d'un système cryptographique, c'est-à-dire la facilité avec laquelle plusieurs mises en applications de ce système peuvent interagir. Pour faciliter l'interopérabilité et contribuer à la confiance générale des non initiés, les gens qui travaillent dans les milieux cryptographiques utilisent le concept de normalisation. La normalisation consiste en un ensemble de règles visant à définir, à simplifier et à uniformiser les caractéristiques d'un système cryptographique ainsi que les méthodes de mise en application de ce dernier de manière à en faciliter l'utilisation et la commercialisation. On retrouve, dans le processus, des séries d'études techniques et de discussions ouvertes dans lesquelles les théoriciens et les praticiens sont appelés à travailler conjointement.

Dans le cas des SCCE, on peut diviser les documents normatifs en deux grandes catégories.

- **Les normes principales.** Les normes principales donnent des spécifications détaillées sur des primitives et des protocoles cryptographiques. On y trouve la description précise d'algorithmes permettant d'effectuer des opérations cryptographiques. Tous les paramètres pour la mise en application sont rigoureusement définis et expliqués. Dans le cas d'une signature électronique de type ECC par exemple, on y retrouverait la liste des courbes pouvant être utilisées, la représentation des points de celles-ci et une description détaillée de chaque étape des algorithmes de construction des clés, de signature et de vérification. Deux personnes qui suivent une même norme principale, obtiennent, en principe, des mises en applications compatibles.

- **Les normes secondaires.** Plusieurs organisations nationales et internationales ont développé des protocoles qui utilisent des systèmes à clés publiques. La plupart de ces protocoles sont construits de manière à ce qu'ils soient indépendants des algorithmes choisis pour la mise en application, permettant ainsi à différents systèmes à clés publiques d'être utilisés. Ces normes secondaires font habituellement référence à une norme principale quand il s'agit de mettre en application les opérations cryptographiques d'un système donné.

Les deux paragraphes suivants présentent une liste – qui ne saurait être exhaustive – des normes principales et secondaires faisant référence à la cryptographie sur courbes elliptiques.

7.1 Normes principales

- **ANSI X9.** (*American National Standards Institute - Financial Services*)
  Les normes ANSI suivantes décrivent la mise en application de la technologie ECC
  - X9 62-1998 *Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm* (ECDSA),
  - X9 63: *Key Agreement and Key Transport Using Elliptic Curve-Based Cryptography*,
  - X9 TG-17 *Public-Key Cryptography for the Financial Services Industry: Technical Guideline on Elliptic Arithmetic*

  La norme X9.62 couvre l'algorithme ECDSA Les deux autres normes sont en cours d'élaboration. La première concerne la gestion des clés symétriques et la seconde est un guide technique sur les mathématiques qui interviennent dans l'utilisation des systèmes à courbes elliptiques.
  `http://www.x9.org/`

- **SECG.** (*Standards for Efficient Cryptography Group*)
  Le SECG a été lancé par *Certicom Corporation* dans le but de faciliter la mise en application de la cryptographie par courbes elliptiques Deux normes ont été publiées sur Internet en septembre 2000
  - SEC 1: *Elliptic Curve Cryptography*, version 1.0 et
  - SEC 2: *Recommended Elliptic Curve Cryptography Domain Parameters*, version 1.0

  Le groupe travaille également sur un certificat X.509 pour ECC
  `http://www.secg.org/`

- **IEEE P1363.** (*Institute of the Electrical and Electronics Engineers*)
  Le projet P1363, *Standard Specifications for Public-Key Cryptography*, a été entériné officiellement comme norme IEEE en février 2000 Le brouillon P1363a *Standard Specifications for Public-Key Cryptography: Additional Techniques* est en cours de construction et sera éventuellement fusionné avec la norme P1363 Ces documents incluent des schémas cryptographiques, de signature et d'échange de clés basés sur ECC.
  `http://grouper.ieee.org/groups/1363/`

- **ISO/IEC.** (*International Standards Organization / International Electrotechnical Commission*)
  Cet organisme a produit les documents suivants:
  - 14888-3 *Digital signatures with appendix - Part 3: Certificate-based*, 20 dé-

cembre 1998.

- 9796-4 *Digital signature schemes giving message recovery - Part 4: Discrete logarithm based mechanisms*, mai 1999 et
- 15946: *Cryptographic techniques based on elliptic curves*

La norme 14888-3 donne les spécifications du protocole ECDSA. La norme 9796-4 décrit une technique de signature électronique basée sur ECC permettant de reconstruire le message signé à partir de la signature. Le dernier document qui est toujours en cours d'élaboration traite de plusieurs techniques cryptographiques sur courbes elliptiques, dont, entre autres, des schémas de signature, des schémas de cryptage et des protocoles d'échange de clés
`http://www.iso.ch`

- **FIPS 186-2.** (*Federal Information Processing Standards*)
  Le *National Institute of Standards and Technology* (NIST) a produit en janvier 2000 la norme FIPS 186-2 intitulée *Digital Signature Standard* (DSS). On y traite des algorithmes de signature DSA, RSA et ECDSA. Les deux premiers sont basés sur la norme ANSI X9.31 et le dernier sur la norme ANSI X9.62. On trouve à l'annexe 6 du document des recommandations quant aux courbes elliptiques pouvant être utilisées dans les communications gouvernementales américaines
  `http://www.nist.gov/`

- **RFC.** (*Request for Comments*)
  Les documents RFC sont des notes techniques concernant l'Internet et dont les débuts remontent à 1969. Les notes officielles suivantes donnent des spécifications sur ECC:
  - 2409: *The Internet Key Exchange* (IKE), novembre 1998 et
  - 2412: *The OAKLEY Key Determination Protocol*, novembre 1998.

  On trouve dans ces documents des descriptions de protocoles et des recommandations quant aux courbes elliptiques pouvant être utilisées.
  `http://www.rfc-editor.org/`

- **PKCS #13.** (*Public-Key Cryptography Standards*)
  Le document PKCS #13 *Elliptic Curve Cryptography Standard* est toujours en cours d'élaboration. Il fait partie d'une famille de normes cryptographiques produites par la compagnie *RSA Laboratories*. Son but est de couvrir les aspects suivants de la cryptographie sur courbes elliptiques: construction et validation des paramètres et des clés, signature électronique, cryptage, échange de clés et ASN.1 (*Abstract Syntax Notation One*) pour les paramètres, les clés et les schémas d'identification. Les protocoles PKCS sont basés sur les normes ANSI et IEEE
  `http://www.rsasecurity.com/rsalabs/pkcs/`

Les normes principales présentées ci-haut ne sont évidemment pas totalement indépendantes les unes des autres. Certaines, comme les normes ISO, sont plus permissives et plus générales, alors que d'autres, comme les normes FIPS, sont beaucoup plus restrictives et précises. Par exemple, une mise en application du protocole ECDSA selon la norme FIPS 186-2 est aussi conforme à la norme ANSI X9.62. Cependant, la réciproque n'est pas vraie en général. La norme ANSI X9.62 est donc plus permissive que la norme FIPS 186-2. Dans le cas du protocole ECDSA, on obtient la hiérarchie suivante

$$\text{FIPS 186-2} < \text{ANSI X9.62} < \text{IEEE P1363} < \text{ISO/IEC 14888-3}.$$

7.2 Normes secondaires

- **RFC.** (*Request for Comments*)
  Outre les deux normes principales RFC mentionnées dans le paragraphe précédent, plusieurs autres documents laissent une place explicite pour l'utilisation de ECC. Ces documents sont

  - 1824: *The Exponential Security System (TESS): An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange (E I S S - Report 1995/4)*, août 1995,
  - 2093: *Group Key Management Protocol (GKMP) Specification*, juillet 1997,
  - 2440: *OpenPGP Message Format*, novembre 1998;
  - 2535: *Domain Name System (DNS) Security Extensions*, mars 1999;
  - 2785: *Methods for Avoiding the "Small-Subgroup" Attacks on the Diffie-Hellman Key Agreement Method for Secure Multipurpose Internet Mail Extension (S/MIME)*, mars 2000;
  - 2801. *The Internet Open Trading Protocol* (IOTP), version 1.0, avril 2000 et
  - 2802 *Digital Signatures for the v1.0 Internet Open Trading Protocol*, avril 2000

  Ces deux dernières notes fournissent un cadre d'interopérabilité entre différents systèmes de paiements électroniques comme *eCheck*, *Secure Electronic Transaction* (SET), *Mondex*, *CyberCoin* et *GeldKarte* en encapsulant ces dernières dans une structure commune. La norme IOTP permet l'utilisation de l'algorithme de signature ECDSA
  `http://www.rfc-editor.org/`

- **IETF.** (*Internet Engineering Task Force*)
  L'IETF est un regroupement international de chercheurs, de concepteurs, de vendeurs et d'opérateurs de réseaux concernés par l'évolution d'Internet. Certains des documents préliminaires produits par le groupe sont liés au système ECC. Notons

entre autres:

- *Internet Protocol Security (IPSec)· IKE Authentication Using ECDSA*, 15 mars 2001,
- *IPSec Additional ECC Groups For IKE*, 15 mars 2001,
- *Transport Layer Security (TLS)· ECC Cipher Suites for TLS*, 15 mars 2001;
- *S/MIME· Use of ECC Algorithms in Cryptographic Message Syntax (CMS)*, 12 mars 2001,
- *Public Key Infrastructure X 509 (pkix)· Representation of Elliptic Curve Digital Signature Algorithm (ECDSA) Keys and Signatures in Internet X 509 Public Key Infrastructure Certificates*, juin 1999,
- *ECDSA with Extensible Markup Language (XML) Signature Syntax*, 20 mars 2001,
- *Elliptic Curve KEYs and SIGs in the DNS*, janvier 2001, et
- *Transmission Control Protocol (TCP) Connection Migration*, novembre 2000.

`http://www.ietf.org/`

- **ATM Forum.** (*Asynchronous Transfer Mode Forum*)
  Ce groupe de travail a rédigé un document intitulé *ATM Security Specification, Version 1 0, February 1999* qui traite des mécanismes de sécurité pour les réseaux en mode de transfert asynchrone. On y trouve des spécifications concernant les services de confidentialité, d'authentification, d'intégrité et de contrôle d'accès. Parmi les algorithmes supportés par cette norme, on trouve des variantes de ECDSA et de ECKAS-DH (*Elliptic Curve Key Agreement Scheme - Diffie-Hellman*)
  `http://www.atmforum.com/`

- **FSTC.** (*Financial Services Technology Consortium*)
  Cette organisation s'implique dans les services financiers électroniques. Elle a développé, entre autres, le système *eCheck* permettant de produire des chèques électroniques. La cryptographie par courbes elliptiques fait partie des spécifications FSML (*Financial Service Markup Language*) produites par le groupe
  `http://www.fstc.org/`

- **CDPD.** (*Cellular Digital Packet Data*)
  La norme CDPD permet d'accéder à Internet et autres réseaux utilisant la technologie IP (*Internet Protocol*) à l'aide d'une communication sans fil. La cryptographie par courbes elliptiques est utilisée dans le processus d'échange de clés
  `http://www.wirelessdata.org/`

- **ReFLEX.**
  ReFLEX est un protocole de radiomessagerie bidirectionnelle développé par Mo-

P517601.PDF [Page: 56 of 64]

torola.
http://www.motorola.com/MIMS/MSPG/FLEX/

- **WAP WTLS.** (*Wireless Applications Protocol - Wireless Transport Layer Security*)
  WAP est une collection de spécifications ouvertes permettant aux téléphones cellulaires et aux terminaux sans fil d'avoir un accès sécuritaire à Internet et à d'autres services. La norme WAP WTLS, dont la dernière version 1.2.1 fut publiée en juin 2000, permet l'utilisation de protocoles basés sur la cryptographie par courbes elliptiques.
  http://www.wapforum.org/

- **ANSI ASC X12 & UN/EDIFACT.** (*American National Standards Institute Accredited Standards Committee X12 & United Nations / Electronic Data Interchange for Administration, Commerce and Transport*)
  Le groupe de travail sur la norme internationale d'échange électronique de données a entamé un processus dans le but d'inclure ECC parmi les techniques cryptographiques supportées dans la norme EDIFACT.
  http://www.x12.org/
  http://www.edifact-wg.org/

P517601.PDF [Page: 57 of 64]

8 Conclusion

La cryptographie à clés publiques revêt une grande importance aujourd'hui. Elle permet, dans le monde électronique, d'offrir une vaste gamme de services, dont ceux de confidentialité, d'intégrité, d'authentification et de non répudiation. Le système à clés publiques le plus connu est sans aucun doute le système RSA. Sa sécurité est basée sur la difficulté à résoudre le problème de factorisation, c'est-à-dire à trouver les facteurs premiers d'un entier composé. Il y a aussi les systèmes basés sur le problème du logarithme discret. Dans ce cas, la sécurité des schémas cryptographiques est basée sur la difficulté à trouver, pour deux éléments donnés α et β d'un groupe multiplicatif cyclique, l'entier x satisfaisant l'équation $\alpha^x = \beta$. La cryptographie sur courbe elliptique est un système basé sur le PLD. Alors que les systèmes classiques utilisent les groupes multiplicatifs provenant des corps finis, ECC utilise le groupe additif d'une courbe elliptique sur un corps fini. Ces groupes offrent l'avantage d'être nombreux en comparaison aux groupes multiplicatifs de corps finis. Aussi, la résolution du PLD étant plus difficile dans les groupes sur courbes elliptiques que dans les groupes de corps finis, on obtient une plus grande sécurité par bit de clé.

La cryptographie par courbes elliptiques est maintenant considérée comme une technologie mature et offrant des avantages indéniables sur d'autres systèmes. L'avenir de ECC est donc prometteur, en particulier dans le monde des communications sans fil où l'on fait face à des contraintes de capacité de stockage, de largeur de bande et de vitesse d'exécution. Au plan international, la promotion du système ECC se fait par l'entremise de compagnies comme *Certicom Corp* et d'organismes normatifs reconnus comme ISO/IEC, ANSI X9, IEEE et RFC. Le service de signature électronique ECDSA et celui d'échange de clés sont de plus en plus présents dans des protocoles internationaux d'échange électronique d'information.

En terminant, mentionnons que la cryptographie par courbe elliptique est un domaine où la recherche fondamentale est toujours très active. Par exemple, des recherches sont en cours sur la résolution du PLD, sur des méthodes d'analyse de puissance et de temps, sur le développement de techniques permettant d'effectuer le cryptage et la signature simultanément, sur des techniques faisant appel aux courbes hyper-elliptiques, etc... Il faut bien sûr rester à l'affût d'éventuels développements.

P517601.PDF [Page: 58 of 64]

Références

[1] I. N. Herstein. **Topics in Algebra**. Xerox College Pub., Lexington, Massachusetts, 2e édition, 1975

[2] T W Hungerford **Algebra** Holt, Rinehart and Winston. New York. 1974

[3] R Lidl et H. Niederreiter. **Introduction to finite fields and Their Applications**. Cambridge University Press, Cambridge, England, 1994

[4] R C Mullin, I M. Onyszchuk, S.A Vanstone et R.M Wilson **Optimal normal bases in GF(p^n)**. *Discrete Applied Math* , 22 :149–161, 1988/1989

[5] D. W Ash, I F Blake et S. A Vanstone **Low Complexity Normal Bases**. *Discrete Applied Math* , 25 :191–210, 1989.

[6] S. Gao. **Normal Bases over Finite Fields**. Ph D thesis in combinatorics and optimization, University of Waterloo, Ontario, Canada. 1993

[7] M. Rosing. **Implementing Elliptic Curve Cryptography**. Manning, november 1998.

[8] Andreas Enge **Elliptic curves and their applications to cryptography : an introduction**. Kluwer Academic Publishers, 1999

[9] G Agnew, R. Mullin, I. Onyszchuk et S. Vanstone **An implementation for a fast public-key cryptosystem** *Journal of Cryptology*. 3 :63–79, 1991.

[10] C. Schnorr. **Efficient signature generation by smart cards**. *Journal of Cryptology*. 4 :161–174, 1991

[11] K McCurley. **A key distribution system equivalent to factoring** *Journal of Cryptology*, 1 :95–105. 1988.

[12] N. Koblitz **Elliptic curve cryptosystems** *Mathematics of Computation*, 48 :203–209. 1987

[13] V. Miller **Uses of elliptic curves in cryptography** *Advances in Cryptology - CRYPTO '85*, 218 :417–426, 1986.

[14] N. Koblitz. **Hyperelliptic cryptosystems** *Journal of Cryptology*. 1 :139–150, 1989

[15] J Pollard **Monte Carlo methods for index computation mod p** *Mathematics of Computation*. 32 :918–924, 1978.

[16] P van Oorschot et M Wiener **Parallel collision search with cryptanalytic applications** *Journal of Cryptology*, 32 :1–28. 1999

[17] R Gallant, R Lambert et S. Vanstone **Improving the parallelized Pollard lambda search on binary anomalous curves**. À paraitre dans *Mathematics of Computation*.

[18] M. Wiener et R. Zuccherato. **Faster attacks on elliptic curve cryptosystems** *selected Areas in Cryptography*, 1556 :190–200, 1999

[19] R. Silverman et J Stapleton, 1997 Contributions au groupe de travail ANSI X9F1

P517601.PDF [Page: 59 of 64]

[20] L. M. Adelman. **A subexponential algorithm for the discrete logarithm problem with applications to cryptography**. *Proceedings of the IEEE 20th Annual Symposium on Foundations of Computer Science*, pages 55–60, 1979.

[21] M. E Hellman et J. M. Reyneri. **Fast computation of discrete logarithms in $GF(q)$**. *Advances in Cryptology - Proceedings of Crypto 82*. pages 3–13, 1983.

[22] D. Coppersmith, A. M Oldzyko et R. Schroeppel. **Discrete logarithms in $GF(p)$** *Algorithmica 82*, 1 :1–15, 1986.

[23] L. M. Adelman. **The function field sieve** *Algorithmic number theory*, 877 108–121, 1994

[24] L M. Adelman et J DeMarrais. **A subexponential algorithm for discrete logarithms over all finite fields** *Mathematics of Computation*, 61 :1–15, 1993

[25] SECG. **SEC 1, Elliptic Curve Cryptography, v1.0**, Septembre 2000 Disponible sur Internet `http://www.secg.org/`

[26] A. Menezes, P. van Oorschot et S Vanstone. **Handbook of Applied Cryptography** CRC Press, Inc , 1997.

[27] D. Boneh et R. Lipton. **Algorithms for black box fields and their application to cryptography** *In Proceedings Crypto '96*, 1109 283–297, 1996.

[28] W. Diffie et M E Hellman. **New directions in cryptography** *IEEE Transactions on Information Theory*, 22 :644–654, 1976

[29] A Menezes, T Okamoto et S. Vanstone. **Reducing elliptic curve logarithms to logarithms in a finite field**. *IEEE transactions on Information Theory*. 39 1639–1646, 1993.

[30] N. Koblitz. **Elliptic curve implementations of zero-knowledge blobs** *Journal of Cryptology*, 4(3) :207–213, 1991

[31] R. Balasubramanian et N. Koblitz. **The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm**. *Journal of Cryptology*, 11 114–145, 1998

[32] N. Smart **The discrete logarithm problem on elliptic curves of trace one** *Journal of Cryptology*, 12 :193–196, 1999.

[33] P Gaudry, F. Hess et N Smart. **Constructive and destructive facets of Weil descent on elliptic curves**. Prépublication, disponible sur Internet `http://www.hpl.hp.com/techreports/2000/HPL-2000-10.html`, janvier 2000

[34] S Pohlig et M Hellman **An improved algorithm for computing logarithms over GF(p) and its cryptographic significance**. *IEEE Transactions on Information Theory*, 24 .106–110, 1978.

P517601.PDF [Page: 60 of 64]

Liste des abréviations, acronymes et sigles

Acronyme	Définition	Page
ANSI	*American National Standards Institute*	39
ASC	*Accredited Standards Committee*	43
ASN 1	*Abstract Syntax Notation One*	40
ATM	*Asynchronous Transfer Mode*	42
CDPD	*Cellular Digital Packet Data*	42
CMS	*Cryptographic Message Syntax*	42
DNS	*Domain Name System*	41
DSA	*Digital Signature Algorithm*	1
DSS	*Digital Signature Standard*	40
ECC	*Elliptic Curve Cryptography*	35
ECDSA	*Elliptic Curve Digital Signature Algorithm*	29
ECIES	*Elliptic Curve Integrated Encryption Scheme*	31
ECDHS	*Elliptic Curve Diffie-Hellman Scheme*	33
ECKAS-DH	*Elliptic Curve Key Agreement Scheme – Diffie-Hellman*	42
FIPS	*Federal Information Processing Standards*	40
FSML	*Financial Service Markup Language*	42
FSTC	*Financial Services Technology Consortium*	42
GKMP	*Group Key Management Protocol*	41
IEC	*International Electrotechnical Commission*	39
IEEE	*Institute of the Electrical and Electronics Engineers*	39
IETF	*Internet Engineering Task Force*	41
IKE	*The Internet Key Exchange*	40
IOTP	*Internet Open Trading Protocol*	41
IP	*Internet Protocol*	42
IPSec	*Internet Protocol Security*	42
ISO	*International Standards Organization*	39
NIST	*National Institute of Standards and Technology*	40
PKCS	*Public-Key Cryptography Standards*	40
PKIX	*Public Key Infrastructure X 509*	42
PLD	Problème du logarithme discret	1
RFC	*Request for Comments*	40
RSA	Rivest-Shamir-Adleman	1
S/MIME	*Secure Multipurpose Internet Mail Extension*	41
SCCE	Systèmes cryptographiques sur courbes elliptiques	1
SECG	*Standards for Efficient Cryptography Group*	29
SET	*Secure Electronic Transaction*	41
TCP	*Transmission Control Protocol*	42
TESS	*The Exponential Security System*	41

P517601.PDF [Page: 61 of 64]

Acronyme	Définition	Page
TLS	*Transport Layer Security*	42
UN/EDIFACT	*United Nations / Electronic Data Interchange for Administration, Commerce and Transport*	43
WAP	*Wireless Applications Protocol*	43
WTLS	*Wireless Transport Layer Security*	43
XML	*Extensible Markup Language*	42

SANS CLASSIFICATION

COTE DE SÉCURITÉ DE LA FORMULE
(plus haut niveau du titre, du resume ou des mots-clefs)

FICHE DE CONTRÔLE DU DOCUMENT

1 PROVENANCE (le nom et l'adresse)	2 COTE DE SÉCURITÉ (y compris les notices d'avertissement, s'il y a lieu)
Centre de Recherches pour la défense Ottawa 3701 avenue Carling Ottawa, Ontario, K1A 0Z4	SANS CLASSIFICATION

3 TITRE (Indiquer la cote de securité au moyen de l'abréviation (S, C, R ou U) mise entre parentheses, immédiatement apres le titre)
Courbes elliptiques et cryptographie (U)

4 AUTEURS (Nom de famille, prenom et initiales Indiquer les grades militaires, ex Bleau, Maj Louis E)
Rostand, Jérémie

5 DATE DE PUBLICATION DU DOCUMENT (mois et annee)	6a NOMBRE DE PAGES	6b NOMBRE DE REFERENCE
Octobre 2001	viii + 48	34

7 DESCRIPTION DU DOCUMENT (La catégone du document, par exemple rapport, note technique ou mémorandum Indiquer les dates lorsque le rap couvre une période définie)
Mémorandum technique

8 PARRAIN (le nom et l'adresse)
Section d'opérations d'information, CRDO, Ottawa

9a NUMERO DU PROJET OU DE LA SUBVENTION (Spécifier si c'est un projet ou une subvention)	9b NUMERO DE CONTRAT
5bf27	

10a NUMÉRO DU DOCUMENT DE L'ORGANISME EXPEDITEUR	10b AUTRES NUMÉROS DU DOCUMENT
DREO TM 2001-095	N/A

11 ACCÈS AU DOCUMENT (Toutes les restrictions concernant une diffusion plus ample du document, autres que celles inhérentes à la cote de sécurité

- ☒ Diffusion illimitee
- ☐ Diffusion limitée aux entrepreneurs des pays suivants (specifier)
- ☐ Diffusion limitée aux entrepreneurs canadiens (avec une justification)
- ☐ Diffusion limitée aux organismes gouvernementaux (avec une justification)
- ☐ Diffusion limitée aux ministères de la Défense
- ☐ Autres

12 ANNONCE DU DOCUMENT (Toutes les restrictions à l'annonce bibliographique de ce document Cela correspond, en principe, aux donnees d'ac au document (11) Lorsqu'une diffusion supplémentaire (à d'autres organismes que ceux precises à la case 11) est possible, on pourra élargir le ce de diffusion de l'annonce)
Annonce complete illimitee

SANS CLASSIFICATION

COTE DE LA SÉCURITÉ DE LA FORMULE
(plus haut niveau du titre, du resumé ou des mots-clefs)

13. SOMMAIRE (Un résumé clair et concis du document Les renseignements peuvent aussi figurer ailleurs dans le document Il est souhaitable sommaire des documents classifies soit non classifié Il faut inscrire au commencement de chaque paragraphe du sommaire la cote de applicable aux renseignements qui s'y trouvent, à moins que le document lui-même soit non classifié Se servir des lettres suivantes (S), (C) (U) Il n'est pas necessaire de fournir ici des sommaires dans les deux langues officielles à moins que le document soit bilingue)

Les techniques de cryptographie à clés publiques sont largement utilisees aujourd'hui pour la protection de donnees électroniques L'une de ces tech qui est particulièrement prometteuse, est basée sur la theorie des courbes elliptiques Ce document à pour but de décrire la cryptographie sur elliptiques (ECC)

Nous commencerons par un bref rappel des notions de structures algébriques élémentaires Puis, nous définirons les concepts de courbes elliptiqu groupes sur courbes elliptiques, et nous verrons comment ces derniers peuvent être utilisés pour construire un système cryptographique à cles pu Nous discuterons ensuite de certaines courbes elliptiques particulieres qu'il faut eviter en cryptographie en raison de leur securité réduite Finaleme terminerons par une revue des normes internationales qui traitent ou font référence a ECC

14 MOTS-CLÉS, DESCRIPTEURS OU RENSEIGNEMENTS SPECIAUX (Expressions ou mots significatifs du point de vue technique, qui caracte document et peuvent aider a le cataloguer Il faut choisir des termes qui n'exigent pas de cote de sécurité Des renseignements tels que le mo l'équipement, la marque de fabrique, le nom de code du projet militaire, la situation géographique, peuvent servir de mots-clés Si possible, choisir des mots-clés d'un thésaurus, par exemple le "Thesaurus of Engineering and Scientific Terms (TESTS)" Nommer ce thésaurus Si l'on pas trouver de termes non classifiés, il faut indiquer la classification de chaque terme comme on le fait avec le titre)

courbes elliptiques, cryptographie, signature électronique, cryptage, echange de clés, normes, ECC

SANS CLASSIFICATION

COTE DE SÉCURITÉ DE LA FORMULE
(plus haut niveau du titre, du résume ou des mots-clefs)

Defence R&D Canada
is the national authority for providing
Science and Technology (S&T) leadership
in the advancement and maintenance
of Canada's defence capabilities.

R et D pour la défense Canada
est responsable, au niveau national, pour
les sciences et la technologie (S et T)
au service de l'avancement et du maintien des
capacités de défense du Canada.

#517601

CA020864

DEFENCE R&D DÉFENSE

www.drdc-rddc.dnd.ca